

COMPUTERWORLD.

THE NEWSPAPER FOR IT LEADERS • WWW.COMPUTERWORLD.COM

JULY 15, 2002 • VOL. 36 • NO. 29 • \$5 COPY

KNOWLEDGE CENTER SECURITY



The Security Action Plan

SPECIAL REPORT

Find out what steps you should take now to

improve corporate security, as well as how to get the

ONLINE EXCLUSIVE

Q&A: The security chief at IBM Global Services discusses corporate IT security, biometrics and homeland security.

QuickLink: 3777
www.computerworld.com

biggest bang from your security buck.

SOME HIGHLIGHTS:

- **An exclusive survey** on rogue wireless LAN access points.
- **Tricks of the computer** forensics trade.
- **Field Report** on virtual private networks.
- **Futurists predict** federal security audits and "security malpractice" lawsuits.

STORIES BEGIN ON PAGE 23.

WORLD.COM USERS ASK, "WHAT IF...?"

Diversification, backup planning come to fore

BY PATRICK THIBODEAU
WASHINGTON

The contingency planning that IT manager Barry Brunetto de-

veloped for his company. Blount International Inc. covers a lot of scenarios, including failed circuits and earthquakes. But he never imagined that a company of WorldCom Inc.'s stature could be a disaster, and Brunetto is now looking for a

safety net for his data services. He's not alone.

Brunetto, the Portland, Ore.-based director of information systems at the sporting goods and power equipment maker, thought he had a viable business-contingency protection strategy in place: restricting business agreements to "Tier I" companies — the most reliable ones. That was then.

"One of the reasons we deal with Tier 1 vendors is the sta-

WorldCom, page 16

WAR ON TERROR AIDS IT MARKET

Vendors vie for piece of homeland security pie

BY DAN VESTON

The war on terrorism is fueling a much-needed economic boost of the IT market, according to analysts and corporate executives. And slump-weary vendors are scrambling for a piece of the action.

Of the \$38 billion earmarked for homeland security in the Bush administration's fiscal 2003 budget proposal, as much

as \$6.5 billion could be spent on new cybersecurity programs, estimated John Pescatore, an analyst at Stamford, Conn.-based Gartner Inc.

The potential windfall has many traditional IT companies expanding their offerings from strictly commercial applications to encompass homeland security.

The Bush administration's focus on using the nation's IT brain trust to tackle homeland security has attracted a wide range of mainstream IT companies, such as American Management Systems Inc., IBM, MicroStrategy Inc., Oracle Corp., Symbol Technologies

War on Terror, page 57

L00L00L00L00L00L00L00L00L00L00L00L
SNDSTFTB 000000N/TOMS-DIRTY 481BC
481BC/PDZQAP986C NOV 82 001 7431
PREMIEST 83
PD BOX 964 65-8
FBI ARREST NY 481BC-PDNY



9:01 AM:
2,500 EMPLOYEES.
9:02 AM:
COMPANY MERGES.
9:03 AM:
18,002 EMPLOYEES.
(ALL IN ALL, JUST ANOTHER DAY AT THE OFFICE.)

In business, change can happen with a vengeance. But you can also adapt with a vengeance, if you have the right tools. mySAP™ HR helps your organization align and leverage people quickly to meet business objectives. It also integrates all aspects of Human Capital Management with the rest of your business, so you can analyze and measure performance or need in real time. Which could have a real impact on your bottom line. Visit sap.com/solutions/hr or call us at 800 880 1727 for details.

THE BEST-RUN E-BUSINESSES RUN SAP





Can your software help keep your business up and running no matter what?
Ours can.

Your company's infrastructure is far too important to risk. That's why our full range of business continuity solutions ensures you're able to handle anything. BrightStor™ storage solutions provide the most comprehensive data backup and recovery. eTrust™ security solutions provide total protection for your entire enterprise, not just pieces. And Unicenter® infrastructure software keeps your whole business up and running 24 x 7. As your business grows and becomes more complex, you need software solutions you can rely on. You may still not know what's coming. But you will know you're prepared.

ca.com/continuity

Business Continuity Solutions



Computer Associates™

COMPUTERWORLD THIS WEEK

NEWS 6

6 Southwest Airlines navigates a turbulent post-Sept. 11 travel market with the help of business intelligence software.

7 Novell's road map for directory services spotlights a plan to extend identity management to Web services technologies.

8 Oracle goes head to head with Microsoft in the messaging market, unveiling collaboration software with links to Oracle's databases.

12 Microsoft customers gain an ally in contract negotiations with the vendor.

14 Itanium 2 won't be an overnight sensation, because software that takes advantage of its 64-bit technology is hard to find.

57 2-D bar code readers may be required equipment for businesses that want to scan driver's licenses.

OPINIONS

Maryfran Johnson	20
Pimm Fox	20
Don Gillmor	21
Frank Hayes	58
Letters	21

How to Contact CW	56
Company Index	56
Shark Tank	56

ONLINE

The Importance of ROI

How critical are ROI analyses in your work? Check out a reader's inquiry in our online discussion forum.

QuickLink: #2329

What's a QuickLink?

On some pages in this issue, you'll see a QuickLink code pointing to additional, related content on our Web site. Just enter that code into our QuickLink box online, which you'll see at the top of each page on our site.

BREAKING NEWS

For breaking news, updated twice daily, visit

QuickLink: #610
www.computerworld.com

KNOWLEDGE CENTER SECURITY

SPECIAL REPORT

23 The Security Action Plan

EDITOR'S NOTE: Today's IT security crisis is every bit as big as the Y2K problem — except that it doesn't have an immovable deadline. This special report provides a to-do list that ranges from managing patches and assembling an incident response team to securing wireless LANs.

25 The Story So Far A fast-paced history of IT security and disaster recovery, in which our IT heroes do battle against trojans, the Morris worm, Russian hackers, power outages and even earthquakes and hurricanes.



26 ROI: Like every other kind of IT investment, security projects must demonstrate their business value. Here's a step-by-step guide to costing costs and getting the greatest returns.

28 Manage Those Patches! New security software is making it easier to distribute and identify new patches and prioritize installation remains elusive and costly for companies.

ONLINE: When it comes to a complete product for patch management, no single vendor meets all the needs of most IT buyers. QuickLink: 30013

32 Build a Response Team A computer incident response team's mission is to orchestrate a speedy and organized company-wide response to a threat. While the goals of most CIRTs are the same, there are different approaches to assembling the team.

34 Let the Pros Investigate Forensics is a specialized discipline that's fast becoming mandatory for companies that need to show that computer crimes don't go unsolved or unpunished.

ONLINE: Assisting in a forensics investigation can be a complicated business, but there are resources available to help. QuickLink: 30848

36 Watch Out for Wireless Rogues Enterprise IT managers need to develop comprehensive wireless LAN management policies in order to battle the proliferation of rogue access points.

ONLINE: Three products for detecting unauthorized access points on wireless LANs. QuickLink: 30856



38 Put Your IT Eggs in Different Baskets Learn about four approaches that major companies are using to quickly recover or even seamlessly continue doing business when disaster strikes.

ONLINE: Before a particular system goes down, determine the impact it will have on people, technology and processes. QuickLink: 30663

40 QuickStudy: Denial-of-service attacks are an old problem, but a few new twists make them even nastier.

43 Opinion: The way to thwart cyberterrorists is to stay one step ahead of them in finding vulnerabilities, says columnist Nicholas Petreley.

44 Field Report: Virtual private networks are useful security tools that have gained a reputation for being difficult to implement and manage. But today's VPN offerings go a long way toward ease of use.

46 Careers: A roundup of skills, training and salary information for IT security professionals. **ONLINE:** One security engineer offers his tips for staying a step ahead of the hacker community. QuickLink: 30625



47 The Next Chapter Pundits predict the rise of "security malpractice" lawsuits, federal security audits and sluggish growth for smart cards.

HOW EXECUTIVES TALK ABOUT SECURITY TRENDS

The security head at IBM Global Services describes services in demand, the future of biometrics and IBM's work on intelligence sharing. QuickLink: 3111

IT SECURITY CASE STUDIES

How IT managers deal with challenges such as recovering from laptop crashes and monitoring all of those security sensors. QuickLink: 3116

HOW BUSINESS-DRIVEN SYSTEMS CHANGE

The increasing detection systems of the future are likely to be hybrids of signature-based and anomaly-based technologies. QuickLink: 3099

AT DEADLINE

Microsoft Rejects Its Own Dog Food...

Microsoft Technology Inc., a Sunnyvale, Calif.-based company that makes several and virtual private networks hardware and software, announced last week that Microsoft Corp.'s SQL Labs, the unit that works on SQL Server, is using Microsoft's SQL Server security appliance to defend its network against Code Red, Nimda and other worm attacks. The choice was made despite the fact that Microsoft already sells its own security product, Microsoft Internet Security and Acceleration Server, which is touted as a defense against worms. Microsoft declined to comment beyond a SQL network engineer's endorsement of the Microsoft product.

... And Details CRM Suite for .Net

Microsoft last week detailed a plan to release in the fourth quarter Web-based customer relationship management (CRM) software based on its .Net platform. The suite will provide a Web-based system for managing accounting, human resources, supply chain and customer relationships at businesses with 25 to 500 employees, Microsoft said. It will be offered as a hosted service and as a product that companies can deploy on their own servers.

Short Takes

AOL TIME WARNER INC. confirmed Friday that it has hired an executive search firm to help find a new head for its flagging AMERICA ONLINE INC. Internet unit. ... **Increasing market share in the server market:** plans behind DELL COMPUTER CORP. boost its earnings estimates for its second fiscal quarter of 2003. ... **ACCENTURE LTD.** narrowly beat revenue and earnings expectations for the third quarter of its 2002 fiscal year. ... **About 27% of developers in China** are currently writing Linux applications, according to a survey of 700 developers by CHINA DATA CORP. in Santa Cruz, Calif.

Southwest Expands Business Tools' Role

Will manage operational data with tools that helped stabilize finances after attacks

BY MARC L. BOWDIE

NEARLY A YEAR after Sept. 11 and the ensuing plunge in airline revenues, Southwest Airlines Co. is so pleased with the performance of its business intelligence applications for financial management that it plans to expand deployment to include flight operations and maintenance.

While some companies have difficulty getting the most out of their very expensive analytic applications, in the middle of a crisis, the Dallas-based airline successfully put its Hyperion Solutions Corp. Essbase online analytical processing (OLAP) application and Pillar budgeting software to the test, according to one of the company's top financial executives. Southwest was able to accurately make financial forecasts to help it prepare adequately for the severe market downturn.

Indeed, Southwest is one of the rare companies that has exploited its business intelligence applications successfully, said Lee Geisbecker, an analyst at Stamford, Conn.-based Gartner Inc.

Key to Success

Southwest's success resulted from its ability to tie its enterprise resource planning applications to its OLAP software and then present relevant financial data and scenarios to its decision-makers.

Typically, companies don't adequately tie their financial applications into an OLAP system, analyze their data and then meaningfully present it to business personnel, but Southwest has proved that it can be done, Geisbecker said.

Right after the terrorist attacks, the airline was operating

"in a world of complete uncertainty," said Mike Van de Ven, vice president of financial planning and analysis at Southwest. "We were asked to give some sort of financial insight for a variety of decisions the company might make."

Prior to the roughly \$1 million installation of Essbase from Sunwayvale, Calif.-based Hyperion in 1999, Southwest Hyperion staff personnel had to write

queries by hand, spend perhaps a half hour running them and then put the figures into spreadsheets for additional analysis, which could take up to four hours. However, Essbase has cut that time to as little as two minutes, said Van de Ven, which means crucial savings for the airline.

After running worst- and best-case scenarios and creating forecasts, Southwest was able to come up with an action plan to stabilize its finances. It helped answer questions like, "How fast would we burn through our cash?" Van de Ven



said. So far, the forecasts have been within 2% of the actual operating numbers, he noted.

Overall, the application has paid for itself through the savings that resulted from automating the data collection processes, Van de Ven said. ■

NCR's Teradata Pricing 'Illogical,' Gartner Warns

New nodes are 25% slower, firm claims

BY JANHUMAR VIJAYAN

Gartner Inc. is cautioning NCR Corp.'s Teradata customers against overpaying for some recently introduced hardware, in response to what the research firm is calling "illogical pricing practices."

The warning relates to a new generation of NCR's monolithic parallel WorldMark servers that were introduced in May.

According to Gartner, the new two-processor nodes that are used in the latest WorldMark 5300 servers provide only 75% of the performance available with the four-processor nodes used in the previous WorldMark 5255 servers. But NCR is insisting on selling the new nodes at the same price as the older nodes, Gartner said.

In an advisory released earlier this month, Gartner analyst Kevin Strunge said NCR's prices "are not in line" with standard industry practice.

"By comparison, recent generations of Hewlett-Packard, IBM and Sun Microsystems high-end Unix servers effectively cut the hardware cost of processing power by increasing the processor speeds by up to 50% with little, if any, increase in price," the advisory noted.

Vickie Farrell, a vice president in NCR's Teradata warehouse group, challenged Gartner's position. "What we sell is a complete solution that includes hardware and software," Farrell said. "The list price on

the box is totally irrelevant. We don't sell off-the-shelf hardware. We sell uniquely configured systems that meet a customer's particular needs."

In fact, she said, when performance is compared, a 5000 server costs 11% less than a 5255 at the same performance level.

The real problem lies in NCR's continued unwillingness to publish list prices on its hardware, Strunge said. Unlike other vendors that have clearly published prices, NCR uses a bundled pricing model that gives customers very little idea about how much they're really paying for their hardware, he said.

"If NCR doesn't separately publish prices for its hardware, how do you know for sure that what you are getting is in fact cheaper" than previous hardware he asked.

NCR's habit of not publishing prices can be troubling, said Mohammad Rifaie, a senior manager of information resource management at Royal Bank of Canada in Toronto.

"This is an area of concern that I have raised with NCR management," he noted. "Teradata is very strong in technology and brings a cost of ownership and total cost of ownership to the table. But I think it will be to their advantage if they publish their prices." ■

“
This is an area of concern that I have raised with NCR management.

MOHAMMAD RIFAIE,
ROYAL BANK OF CANADA

Liberty Alliance to Unveil Single Sign-on Technical Spec

Phase 1 deals with authentication sharing

BY CAROL BLUMA

The Liberty Alliance Project today will reveal its long-awaited technical specifications to help companies set up systems that will let users sign on just once to gain access to a host of password-protected Web sites and services.

But the mere fact that the 40-member-plus consortium, led by Sun Microsystems Inc. and United Air Lines Inc., has finally produced something tangible may impress some industry observers more than the details about the technical specifications it backs, such as the Security Assertion Markup Language (SAML).

"A lot of people had been skeptical, and they didn't really understand what this Liberty Alliance was about," said David Smith, an analyst at Gartner Inc. in Stamford, Conn.

Founded last September, the Liberty Alliance Project promised to create technical specifications that would permit single sign-on and decentralized authentication based on openly available technologies. The initiative created an alternative to Microsoft's Passport system, which authenticates only users who access sites that support Passport.

Both the Liberty Alliance and Microsoft have taken great pains to stress that they don't compete. Bill Smith, Sun's representative to the Liberty Alliance, said last week, "We'd hope that Microsoft or anyone with an interest in identity management would join in the work we're doing."

Meanwhile, Adam Soha, a product manager at Microsoft, said his company could join the alliance, work informally with the group on interoperability standards or simply

work to make sure its Passport system can share information with sites that support the Liberty specifications.

That sort of rhetoric has been going on for months with little movement, but Microsoft now has a real specification to review. "We'll take a look at the spec and figure out what the next steps are," Soha said.

The Project Base

The Liberty specification is based on SAML, an XML-based security standard for exchanging authentication and authorization information, but it will also define extensions to SAML, according to James Kobielus, an analyst at Midvale, Utah-based Burton Group.

LIBERTY ALLIANCE PROJECT AT A GLANCE

FOUNDED: September 2001

OBJECTIVE: To provide a federated network identity system for the Internet that enables single sign-on for consumers and businesses.

MANAGEMENT BOARD: American Express Co., AOL Time Warner Inc., BCE Inc., Citigroup Inc., France Telecom, General Motors Corp., Hewlett-Packard Co., MasterCard International Inc., Natus Corp., NTT DoCoMo, Openwave Systems Inc., RSA Security Inc., Sony Corp., Sun Microsystems Inc., United Air Lines Inc., Vodafone Corp.

Kobielus said the Liberty specs use the basic formats and protocols of SAML and add extensions to support account linking, or "identity federation." "Openque identifiers" traverse the Internet, serving as anonymous IDs to permit users to access other sites, but they don't contain personal account information, he said.

For instance, a user might book a flight on one site and be

linked to other sites for car and hotel reservations, but all of his unique account information would be managed separately by the airline, rental car and hotel companies, Kobielus said.

"Liberty makes it difficult to aggregate personal data across linked accounts," Kobielus said. But users can opt to link their accounts, he added.

Phase 1 of the Liberty specification deals strictly with au-

thentication sharing, according to Sun's Smith. Phase 2 is already under discussion, but no details are available.

How well the Phase 1 spec works in practice remains to be seen. Sun, Novell Inc. and other companies today are expected to pledge to support the Liberty specifications in their respective products.

Also today, about a dozen companies, including Novell, Sun and IBM's Tivoli division, are scheduled to demonstrate SAML-enabled products at a hospitality suite sponsored by the nonprofit Organization for the Advancement of Structured Information Standards.

Gartner's Smith said corporate IT departments will probably want to make their existing systems work in the Liberty environment rather than throw out what they have and buy new products. But that could mean custom coding for their developers, he said. ■

Novell Lays Out Road Map For New Directory Services

But company has yet to specify dates

BY CAROL BLUMA

Novell Inc. today plans to unveil an 18-month road map for its eDirectory server software, dubbed Project Destiny, that outlines its strategy to extend secure identity management to every aspect of Web services.

But while the software maker is drawing analysts' praise for heading in the right direction, so far for the only product that has an expected year's end ship date is the Universal Description, Discovery and Integration (UDDI) server that's being built on its eDirectory server.

"They have a lot of good ideas, and they've had them for a while. But when are they going to deliver?" said Mike Neuenchwander, an analyst at Burton Group in Midvale, Utah. "They're trying to jump

the gun and be a thought leader. It's more important for them to be a product leader."

At least with the Web services and UDDI plans, Novell may be running ahead of the demand curve. IT departments have been rushing to build Web services or use public UDDI repositories that can help them find information about how their trading partners want to interact.

The first part of Novell's directory services road map calls for the addition of a server to its eDirectory that will bring user authentication and access control to UDDI registries. That will allow authorized users to add information to and query information from UDDI registries, according to Ed Anderson, director of product management for the company's identity services group.

Anderson said he anticipates that large companies will start to deploy internal UDDI re-

positories next year. He predicted that some will experiment with the federation of their internal repositories so they can share information with business partners. "It will become more prominent in 2004 and forward," he said.

Neuenchwander said the UDDI server represents only "one-sixteenth" of what Novell wants to do through its Destiny road map. "The marketing guys are getting ahead of the engineering guys," he said.

Novell's Plans

A UDDI server, built on Novell's eDirectory, to add authentication and access control to UDDI registries, due by year's end. Native XML and SOAP support in eDirectory.

One management point for user identities doesn't turn multiple applications and services.

A rules-based engine that will help discover information on access to network resources based on their roles in an organization.

A federated system to allow businesses to securely share identity data with their key partners.

No timetable was announced for several key pieces of the plan, other than that they will be delivered next year, according to a Novell spokesman.

Those pieces include native support for XML and the Simple Object Access Protocol (SOAP) in the eDirectory server; a single point of management for user identities drawn from multiple applications and services; a rules-based engine that will help direct management user access to network resources; and a federated system that will allow businesses to securely share identity information with business partners.

Anderson said the initial pieces will be modular add-ons to eDirectory, which is the foundation of Project Destiny.

John Enck, an analyst at Stamford, Conn.-based Gartner Inc., said the real value in Novell's directory services plan will be from policy-based identity management, which will allow more users to be administered by fewer people.

"You're not going to have to burn IT resources for a simple task like adding or maintaining user information in multiple directories," Enck said. ■

FLASHBACK

For background information on the formation of the Liberty Alliance Project, visit us online at www.libertyalliance.org.



Oracle Tries Again With Messaging Wares

Aims to compete against Exchange

BY JENNIFER DRABOT

ORACLE CORP. last week announced back-end collaboration software that the company hopes will compete with Microsoft Corp.'s Exchange.

Oracle Collaboration Suite includes ready-made links to Oracle's 9i databases, unified messaging and calendaring technology from newly acquired Seltzer Inc. in Montreal.

The move is partly intended to prevent Microsoft from controlling the messaging market and being able to dictate how Oracle software will interoperate with Exchange, said Rene Bonvanie, vice president of product marketing at Oracle.

"I think... Lotus is irrelevant in this market," Bonvanie said. "If we don't stand up, Microsoft will gobble up everything, including Lotus, the way they did to Novell a few years ago," said Bonvanie, referring to GroupWise, a messaging product from Novell Inc.

"At the end of the day, two companies will battle it out for predominance, and we think that we have a very serious shot at this," said Bonvanie.

They're Lifting

Not surprisingly, Microsoft and Lotus Software Group executives were somewhat dismissive of the announcement.

"We've been in this market for five, six-plus years. We've done a lot of heavy lifting," said Chris Baker, lead product manager for Exchange at Microsoft. "So they really have, maybe at best, LQ products."

Baker added that Oracle's offering may have strengths that Microsoft doesn't, but it's not a full-featured product. "It's very much a 'me too,'" he said.

Ed Brill, an IBM Software

operations manager, offered similar views. "I have a déjà vu sense," he said. "This is like the ninth time that they've tried to get into the market."

Still, one Notes customer said Oracle's offering is worth considering. Lenox Inc. in Lawrenceville, N.J., is about to switch to Exchange because of the cost of maintenance and the difficulty of integrating Version R4.6 of Notes with Microsoft's Office software. However, the company would have looked at Oracle's new product if that decision hadn't been

made, said Bob Palmer, vice president of IT at Lenox. "To what degree, it's hard to say without understanding [the product]. One of the issues with Oracle is that everything is database-driven, and that requires database licensing. It's a very expensive proposition to get into that ballgame. If they could provide a solution that scales in a cost-effective manner," it may be worth it, he said.

"Microsoft, for better or worse, they allow you to get into various solutions at more reasonable cost," Palmer

added. "You don't have to be a Fortune 500 company to deploy their solutions."

"I don't think most people will rip and replace. But the future is uncertain," said David Ferris, president of Ferris Research Inc. in San Francisco.

The suite has potential, said Michele Rubenstein, a board member of the Messaging Forum of The Open Group in San Francisco. "With Oracle 8i and above, you have the LDAP [Lightweight Directory Access Protocol] connections, and you can tie this into directory services and PKI [public-key infrastructure]," she said. "Oracle has market share on database, and Microsoft has market share on the messaging [client]. From a user perspective, that's the best of both worlds." ■

High-Speed Wireless Service Debuts, Draws Keen Interest

256K service based on IPWireless technology

BY BOB BREWSTER

Next month, the Hyatt Regency Maui in Hawaii will start offering hotel guests a mobile wireless service that blazes along at 256K bit/sec.—four to five times the speed of next-generation high-speed data services provided by U.S. cellular carriers.

Gary Balson, director of engineering at the Hyatt Corp. hotel, said the capital cost of the service is only \$10,000, which was the price of the 25 pocket-size modems that

up into the high-speed service provided by Maui Sky Fiber LLC in Kihei, Maui.

Steve Berkooff, managing director of Maui Sky Fiber, said his system, which will eventually blanket the island of Maui, has a raw throughput of 3M bit/sec. He plans, however, to limit it to 1.2M bit/sec, "because we don't have demand for that kind of speed on Maui."

Maui Sky Fiber plans to offer

both mobile and fixed wireless services on Maui, with prices ranging from \$2.95 per day for guests using the mobile service to \$349.95 per month for a 768K bit/sec. fixed service to enterprise customers, a price Berkooff said compares favorably with cable modem or Digital Subscriber Line rates on the island.

The company offers the service based on the International Universal Mobile Telecom-

munications System standard over a licensed system operating in the 2.5- to 3.6-GHz Multichannel Multipoint Distribution System (MMDS) frequency band. That system has been designated by the Federal Communications Commission for fixed wireless operations delivering video or data.

Berkooff said the key to his operation is technology developed by San Bruno, Calif.-based IPWireless Inc. that takes advantage of multipath

signals, which Chris Gilbert, CEO of IPWireless, said is the Holy Grail of radio frequency engineering. Gilbert said his firm has developed patented software to harness the power of multipath signals for a quantum increase in throughput.

Berkooff said he was initially skeptical about the IPWireless technology. However, not only does it work, but it does so at far lower capital costs than so-called third-generation cellular wireless systems such as those offered by Nokia Corp., he said. Berkooff estimated his capital costs per cell at \$100,000, as opposed to \$250,000 per cell for similar equipment from a vendor such as Espoon, Finland-based Nokia.

Joe Brooks, vice president of sales and market development for the Broadband Solutions division of financially troubled WorldCom Inc., said his company believes in the technology enough to deploy it on its MMDS system in Memphis. Commercial service is slated to start next month.

"I haven't seen anything like IPWireless' technology, which could be a real plus for WorldCom," Brooks said. WorldCom spent \$1 billion for its nationwide MMDS licenses in the late 1990s. Since the IPWireless model is easy for a customer to install, Brooks said, it could

save WorldCom the costs associated with sending out an installation technician.

Analyst Lindsay Schroth at The Yankee Group in Boston called the IPWireless technology "incredible," noting that it gives suppliers and customers a high-speed fixed or portable service in one package. ■

IPWireless vs. Cellular Data

IPWIRELESS

• 256K bit/sec. max. speed

• \$92.95 a day, or \$99.95 a month, for mobile, 256K bit/sec. service with unlimited use

• \$349.95 a month for 768K bit/sec. fixed service with unlimited use

AT&T WIRELESS

• 67K bit/sec. data service

• 20K to 40K bit/sec.

• Up to 5MB per month of data, downloaded for \$20 a month

• Up to 100MB of data downloaded a month for \$100 a month

VERIZON WIRELESS

• CMAA to mobile data service

• 50K to 70K bit/sec.

• \$50 minutes for \$35 per month

• \$300 minutes for \$300 a month

• \$300 minutes for \$300 a month

• \$300 minutes for \$300 a month

• \$300 minutes for \$300 a month

• \$300 minutes for \$300 a month

• \$300 minutes for \$300 a month

• \$300 minutes for \$300 a month

• \$300 minutes for \$300 a month

• \$300 minutes for \$300 a month

FAQ

Frequently asked question | address FAQ

It's the question we hear most frequently: how can you leverage your investment in existing infrastructure but not miss out on the benefits of new technology? Answer: The Sprint network boasts seamless interoperability between IP, frame relay and ATM platforms — just what you need to help take advantage of current systems while migrating to new technology.

Anytime to virtually anywhere connectivity

We're the only telecommunications provider that supports both nationwide wireless and wireline access to your critical data applications. We can help you integrate wireline IP services with the latest wireless always-on, real-time mobile data solutions. The result? Try higher productivity with access to your data anytime you need it — in the office or on the road.

"Any to any" connectivity

We've also engineered a network solution that marries the "any to any" connectivity of IP to the reliability and security of frame relay. It's called Internet Protocol Intelligent Frame Relay (let's just call it IPiFR), and it's based on a flexible router architecture that can run over multiple backbone technologies — a domestic industry first. What this can give you is VPN services that (1) provide meshed connectivity (2) without multiple PVCs (3) while maintaining predictable scalability. In other words, you can add locations and new applications without replacing your existing infrastructure or adding significant costs.

Get more from existing technology and get ready for the latest — another sign of an intelligent network and the people who make it work (for you).



For more answers, visit our complete library of downloadable white papers at sprint.com/whitepapers/13 or call 1-877-604-1844.



BRIEFS

EMC Taps Accenture For Consulting Unit

EMC Corp. last week announced the creation of Information Solutions Consulting, a business unit that it will operate in a five-year pact with Accenture Ltd. The unit is an element of the Hopkinton, Mass.-based company's strategy to remake its business so that 50% of revenue is derived from hardware, 30% from software and 20% from services.

Tools Available for Visual Studio .Net

Microsoft Corp. last week made available educational materials and a tool kit to help developers build applications using the Visual Studio .Net development environment. Also, an integration software development kit enables companies to hook their internally built tools into the Visual Studio .Net environment.

Microsoft Joins LinuxWorld Exhibitors

Microsoft for the first time will sponsor a booth at the LinuxWorld Conference & Expo, to be held next month in San Francisco. The company will display various tools as its embedded operating systems. "I would definitely not treat this as a move [by Microsoft] to open source, but as a way to reach people here to reach," said Pete Houston, senior director of Microsoft's Windows server product management group.

Security Flaw Found In iPlanet Web Server

A security vulnerability in the search features of Sun Microsystems Inc.'s iPlanet Web server can allow attackers to access code of their choice on remote iPlanet servers, according to a security advisory released last week by U.K.-based Net Generation Security Software Ltd. The flaw affects iPlanet Web server Versions 4.1 and 6.0.

California Proceeds Without an IT Dept.

New unit to create plan to deal with procurement, security issues in state

BY MARC L. SONDHI

WITH THE recent demise of a central oversight department, the state of California during the next weeks and months must cobble together procedures to both procure and secure its multibillion-dollar IT systems.

Lacking legislative reauthorization, the state's Department of Information Technology (DOIT) officially ceased to exist July 1, largely because of its role in a controversial database licensing agreement with Oracle Corp.

For now, state agencies must work with the Department of Finance and assume responsibility for their own IT projects.

But Gov. Gray Davis also created a new unit, the Technology Oversight and Security Unit (TOSU), whose task is to come up with a long-term plan to help manage the state's multibillion-dollar IT investments.

Botched Deal

The DOIT was created in 1996 to oversee high-tech projects throughout California. After earlier controversies, its fortunes declined irreversibly in April, when a scathing report from the state auditor's office laid at its door much of the blame for an approximately \$126 million exclusive database licensing deal with Oracle. The deal, called an enterprise licensing agreement (ELA), would have wound up costing more money than a competi-

Without a DOIT

FOLLOWING THE DEMISE OF CALIFORNIA'S DOIT:

- State agencies will work with the Finance Department to oversee IT-related projects.
- Gov. Gray Davis created the Technology Oversight and Security Unit to develop a long-term plan for managing the state's IT investments.
- The TOSU expects to establish procedures to secure the state network, make bidding processes more fair and promote communication among California IT leaders.

tively bid license, the auditor claimed.

Oracle declined to comment on the DOIT's expiration, and negotiations are under way to rescind the ELA.

The head of the TOSU is Clark Kelso, a law professor at the McGeorge School of Law at

the University of the Pacific in Sacramento. He said his primary task will be to create a road map for what the unit wants to accomplish during the next 18 months.

Among the long-term goals is to make sure all IT purchases are done fairly and ethically, he said. "We want to reduce any appearance of bias or favoritism," Kelso told Computerworld last week.

He also said the state has to do a better job of securing its network, not just because of concerns about cyberterrorism, but also because there was an unauthorized intrusion into a computer at the state's Teale Data Center. The hackers who broke into that system were able to access the Social Security numbers and payroll information of all state employees [QuickLink: 30251].

Among the lessons Kelso said he has learned from the DOIT collapse is the need for IT departments to communicate with other branches in an organization about projects and their worth. "DOIT did not fully engage the legislature and didn't let it know what it was doing and what value they were contributing," he said. ■

where I have worked.

FBI's New CIO Undaunted by Challenges

Says private-sector past will aid in post

BY TODD R. WEISS



Q&A After serving as the worldwide director of information and communications systems for the 11 million-member Church of Jesus

Christ of Latter-day Saints in Salt Lake City since 1990, Darwin A. John will join the government today as the new CIO at the FBI. John, 64, was named to the post last week by FBI Director Robert S. Mueller III to replace Bob John, who served for two years as both CIO and assistant di-

rector for information resources at the agency [QuickLink: 31258].

Since the terrorist attacks on the U.S. last September, IT systems at the FBI and other federal agencies have come into question. Some reports say the systems are antiquated and as much as a decade out of date. Where do you begin to make changes to help the FBI fight terrorism? Director Mueller has stated publicly that there is some catching up to do. He's been clear about that. Some news reports, I believe, may have been exaggerated. I don't see any challenge that isn't doable. Since I haven't yet started at the agency, I haven't been close enough to the FBI's situation to know exactly what

will be needed. I will see when I get there. One specific information management part of my new job will be ensuring that the right information is captured and accessible to those who need access and is not accessible to those who shouldn't have access.

How will your previous experiences help you prepare for and perform your new job at the FBI, where fighting terrorism has become the new mantra? Across my experiences are some systemic things that are very much in common, such as supporting the enterprise and helping to realize its reason for being. My belief is that basic CIO leadership is very transferable across those various kinds of environments

What were your responsibilities in your job with the church? I have been focused on similar things, such as anticipating the future, setting strategic direction and doing development work to put tools and people in place to support the church's mission. My job also entailed minding the shop day to day and ensuring that the infrastructure was reliable and secure.

What are your thoughts as you start this job, knowing how important it may be to the future security of our nation, which is facing the continuing threat of terrorism? At this stage of my life, when most people would probably be thinking about playing golf more often, I've still got some passion about seeing if I can help make a difference for the country. ■

BRIEFS

EMC Taps Accenture For Consulting Unit

EMC Corp. last week announced the creation of Information Solutions Consulting, a business unit that it will operate as a five-year joint venture with Accenture Ltd. The unit is an element of the Hopkinton, Mass.-based company's strategy to remake its business so that 50% of revenue is derived from hardware, 30% from software and 20% from services.

Tools Available for Visual Studio .Net

Microsoft Corp. last week made available educational materials and a tool kit to help developers build applications using the Visual Studio .Net development environment. Also, an integration software development kit enables companies to hook their internally built tools into the Visual Studio .Net environment.

Microsoft Joins LinuxWorld Exhibitors

Microsoft for the first time will sponsor a booth at the LinuxWorld Conference & Expo, to be held next month in San Francisco. The company will display servers such as the embedded operating systems. "I would definitely not treat this as a move [by Microsoft] to open source, but as a way to reach people we have to reach," said Pete Houston, senior director of Microsoft's Windows server product management group.

Security Flaw Found in iPlanet Web Server

A security vulnerability in the search features of Sun Microsystems Inc.'s iPlanet Web server can allow attackers to execute code of their choice on remote iPlanet servers, according to a security advisory released last week by U.K.-based Next Generation Security Software Ltd. The flaw affects iPlanet Web server Versions 4.1 and 6.0.

California Proceeds Without an IT Dept.

New unit to create plan to deal with procurement, security issues in state

BY MARG L. BOWEN

WITH the recent demise of a central oversight department, the state of California during the next weeks and months must cobble together procedures to both procure and secure its multibillion-dollar IT systems.

Lacking legislative reauthorization, the state's Department of Information Technology (DOIT) officially ceased to exist July 1, largely because of its role in a controversial database licensing agreement with Oracle Corp.

For now, state agencies must work with the Department of Finance and assume responsibility for their own IT projects.

But Gov. Gray Davis also created a new unit, the Technology Oversight and Security Unit (TOSU), whose task is to come up with a long-term plan to help manage the state's multibillion-dollar IT investments.

Botched Deal

The DOIT was created in 1996 to oversee high-tech projects throughout California. After earlier controversies, its fortunes declined irreversibly in April, when a scathing report from the state auditor's office laid at its door much of the blame for an approximately \$126 million exclusive database licensing deal with Oracle. The deal, called an enterprise licensing agreement (ELA), would have wound up costing more money than a competi-

Without a DOIT



tively bid license, the auditor claimed.

Oracle declined to comment on the DOIT's expiration, and negotiations are under way to rescind the ELA.

The head of the TOSU is Clark Kelso, a law professor at the McGeorge School of Law at

the University of the Pacific in Sacramento. He said his primary task will be to create a road map for what the unit wants to accomplish during the next 18 months.

Among the long-term goals is to make sure all IT purchases are done fairly and ethically, he said. "We want to reduce any appearance of bias or favoritism," Kelso told Computerworld last week.

He also said the state has to do a better job of securing its network, not just because of concerns about cyberterrorism, but also because there was an unauthorized intrusion into a computer at the state's Teale Data Center. The hackers who broke into that system were able to access the Social Security numbers and payroll information of all state employees [QuickLink: 30251].

Among the lessons Kelso said he has learned from the DOIT collapse is the need for IT departments to communicate with other branches in an organization about projects and their worth. "DOIT did not fully engage the legislature and didn't let it know what it was doing and what value they were contributing," he said. ■

FBI's New CIO Undaunted by Challenges

Says private-sector past will aid in post

BY TODD R. WEISS



After serving as the worldwide director of information and communications systems for the 11 million-member Church of Jesus Christ of Latter-day Saints in Salt Lake City since 1990, Darwin A. John will join the government today as the new CIO at the FBI. John, 64, was named to the post last week by FBI Director Robert S. Mueller III to replace Bob Dies, who served for two years as both CIO and assistant di-

rector for information resources at the agency [QuickLink: 31258].

Since the terrorist attacks on the U.S. last September, IT systems at the FBI and other federal agencies have come into question. Some reports say the systems are antiquated and as much as a decade out of date. Where do you begin to make changes to help the FBI fight terrorism? Director Mueller has stated publicly that there is some catching up to do. He's been clear about that. Some news reports, I believe, may have been exaggerated. I don't see any challenge that isn't doable. Since I haven't yet started at the agency, I haven't been close enough to the FBI's situation to know exactly what

will be needed. I will see when I get there. One specific information management part of my new job will be ensuring that the right information is captured and accessible to those who need access and is not accessible to those who shouldn't have access.

How will your previous experiences help you prepare for and perform your new job at the FBI, where fighting terrorism has become the new mantra? Across my experiences are some systemic things that are very much in common, such as supporting the enterprise and helping to realize its reason for being. My belief is that basic CIO leadership is very transferable across those various kinds of environments

where I have worked.

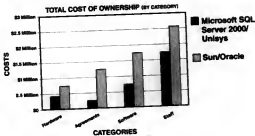
What were your responsibilities in your job with the church?

I have been focused on similar things, such as anticipating the future, setting strategic direction and doing development work to put tools and people in place to support the church's mission. My job also entailed minding the shop day to day and ensuring that the infrastructure was reliable and secure.

What are your thoughts as you start this job, knowing how important it may be to the future security of our nation, which is facing the continuing threat of terrorism? At this stage of my life, when most people would probably be thinking about playing golf more often, I've still got some passion about seeing if I can help make a difference for the country. ■

Figure 4

The Microsoft® SQL Server™ 2000/Unisys BI solution offers \$3.2 million in savings compared with the Oracle/Sun system over a five-year period.



We discovered that the current state of Windows® and Intel solutions offers considerable savings and an attractive alternative to the classic RISC/UNIX solutions for BI implementation.

Source: Walklett Group, February 2002

Page 25

Going with the facts saves money.
microsoft.com/sql/tco Software for the Agile Business.

Microsoft

License Tracker Launched As Microsoft Deadline Looms

Users can get snapshot of software assets
in preparation for contract negotiations

BY CAROL BLIWA

AS MICROSOFT users face a key July 31 licensing deadline, a Canadian firm last week launched its LicenseTracker service to help companies take stock of their Microsoft software in preparation for contract negotiations.

Through the LicenseTracker service from AssetMetric Inc. in Ottawa, corporate users can inventory all of the Microsoft Corp. software running on their desktops, laptops and servers. They can then gain access to Internet-based reports that provide details on the product versions being used and on the build numbers and license keys.

"They can inventory their entire population literally in hours, no matter how centralized and how big they are," said Paul Bodnoff, president and CEO of AssetMetric.

Under Microsoft's old licensing system, many companies didn't keep track of their licenses, and as a result, some of them overbought or underbought when the time came for upgrades, Microsoft CEO Steve Ballmer told *Computerworld* last month.

Now that the company's new Version 6.0 volume licensing program is taking effect, companies are being advised to get an accurate snapshot of their software assets in order to determine which of the new programs, if any, will make sense for them.

"It's really never too late to implement some type of asset management," said Alvin Park,

an analyst at Stamford, Conn.-based Gartner Inc.

However, with just 16 days left before the licensing deadline, Park said he's not sure how much the LicenseTracker service can help.

Rebecca LaBrunner, product manager of worldwide licensing and pricing at Microsoft, said she was unfamiliar with the product and thus unable to comment on its merits.

"We've long said that customers need to understand what software assets they have as

the first step to making an informed licensing decision," she said. "But again, I can't comment as to the results generated by a third-party product."

Users have until July 31 to enroll in Microsoft's new Software Assurance program, which entitles a company to receive the latest versions of Microsoft products during its contract term. Enrolled companies pay 25% of the volume license fee for server software products and 29% for desktop products on an annual basis.

Another option opened until July 31 is Upgrade Advantage, which moves a company to the current version of a Microsoft software product and "grand-

fathers" them for Software Assurance at a later date.

Companies that don't opt for Software Assurance or Upgrade Advantage can simply buy new software licenses, potentially at higher costs, at a later date. Or they can get their Microsoft software licenses as part of a PC hardware purchase.

The LicenseTracker service costs \$2 per seat through July 31. Customers may then opt to upgrade to a full-service subscription. AssetMetric's Impact service costs \$3 per seat for a 30-day subscription; its Project service is \$7 per seat for a 90-day subscription; and the Premier service is \$15 per seat for a full-year subscription. ■

Microsoft Releases Content Management Server Beta

Product features
tool integration,
Web services support

BY CAROL BLIWA

Microsoft Corp. last week released a beta version of its Content Management Server 2002 that features additional authoring and administration capabilities, as well as native support for XML and key Web services standards. Perhaps most notable, however, is its tighter integration with many of Microsoft's other products.

One of the product's key differentiators, for instance, is its integration with the Visual Studio .Net tool set. The company removed developer clients from Content Management Server 2001 in favor of the new tools, said Chris Ramsey, a product manager in Microsoft's .Net Enterprise Server group.

Customers who purchase Visual Studio .Net—which

costs \$1,079 for the professional edition—will get a project wizard to help them build Web sites, saving them from having to write hundreds of lines of code, according to Ramsey.

Ramsey said customers will also get a gallery of content and functionality controls that can be dragged and dropped into applications. An Explorer

panel is designed to help them navigate content in the product's repository and connect it to their Web site projects.

Customers can use Content Management Server without Visual Studio .Net, but Microsoft will recommend that they buy both, Ramsey said.

Other products that have tight hooks into the new Content Management Server include Microsoft's Office software and Application Center server. A new authoring connector lets users create Web content in Microsoft Word and publish it directly to their Web sites via the Content Management Server. Through Application Center, users can manually or automatically schedule the deployment of a Web site throughout the development process, from server to server.

Content Management Server also features tight connections to other Microsoft products, such as Commerce Server and BizTalk Server.

Nicholas Wilford, an analyst at Forrester Research Inc. in Cambridge, Mass., said that integration will help Microsoft compete more aggressively in the enterprise market against competition such as Docu-

On July 31

■ The direct enrollment period for Microsoft's new Software Assurance program ends. Software Assurance entitles customers to the latest version of a Microsoft product. The annual cost is 25% of the volume license fee for a server product and 29% for a desktop product. In order to be eligible, a company must be renewing the most current version of the product. After July 31, a company must purchase new licenses in order to be eligible for Software Assurance.

■ Microsoft's Version 6 volume licensing program ends and the Upgrade Advantage option will no longer be available. Upgrade Advantage entitles a company to its available upgrade of a product and "grandfathers" the company so it's eligible to move to the new Software Assurance program.

KEY FEATURES

Content Management Server 2002

- Direct publishing from Microsoft Word
- Distributed administration
- Native support for XML-based content
- Native support for key Web services standards, such as the Simple Object Access Protocol
- Visual Studio .Net tool set integration
- Drag-and-drop content management server controls
- Wizard for creating Web services
- Source code management system support

mentum Inc., Interwoven Inc. and Vignette Corp. He added that those vendors also recommend various add-on products, such as Java-based application servers and tools that must be purchased separately.

"Microsoft puts a lot of price pressure on these vendors and offers them the quicker and easier to implement," said Wilford. But so far, the competition has landed more customers doing large-scale deployments to date, he said.

Since acquiring the Content Management Server product last year when it bought NetCompass Labs Inc. in Vancouver, British Columbia, Microsoft claims to have substantially increased the number of enterprise-wide deployments of its product.

Jim Murphy, an analyst at AMR Research Inc. in Boston, said Content Management Server 2001 was "fairly lightweight" and that Microsoft won deals largely based on its market strength and viability. He said the new product brings substantial improvements, especially "remonstrable Web services capability," which will lift it "more to a par with enterprise competitors." ■

HEADLINE DETAILS

For more information on Microsoft's licensing deadline, visit our Web site.

QuickLink: 30800
www.computerworld.com

Scalable IP security without breaking the bank.



Meet the Contivity 1000 Series.

How do you harness the power and reach of the Internet in a way that provides security and allows you to scale your network? How do you do this without breaking your IT budget? Look no further than the Contivity™ 1000 family with Secure Routing Technology. The Contivity 1000

Series enables businesses to easily build and manage large VPN networks, using dynamic routing protocols over encrypted tunnels. In addition to support for dynamic routing (RIP and OSPF), it comes fully loaded with remote access VPN, site-to-site VPN, firewall, QoS and bandwidth management. And here's the good part - mix-and-match services. You only buy the services you need initially and turn up the rest when you're ready. It's as easy as turning on a license key. No multiple boxes. No installation hassles. Low TCO. The Contivity 1000 can be installed as a stand-alone IP access gateway (with 5 free VPN tunnels) or behind an existing WAN access device, totally off-loading all security processing. For more information, visit nortelnetworks.com/contivity.

**Starting
under \$1,000**

Metro & Enterprise Networks | Optical Long Haul Networks | Wireless Networks

Nortel Networks, the Nortel Networks logo, the Globespan and Contivity are all trademarks of Nortel Networks. ©2000 Nortel Networks. All rights reserved.

**NORTEL
NETWORKS™**
nortelnetworks.com

BRIEFS

Business Objects to Buy Acta Technology

French software maker Business Objects SA announced an agreement last week to acquire Acta Technology Inc. for close to \$65 million, with plans to join the two companies' data analysis software products. Acta, in Mountain View, Calif., sells software for collecting and organizing data from a variety of systems, including enterprise resource planning and customer relationship management applications.

Former Compaq Exec Replaces EMC CTO

EMC Inc. said last week that its retiring chief technology officer, Jim Rutledge, is being replaced by former Compaq Computer Corp. executive Mark Lewis, who will serve as EMC's CTO and executive vice president of new ventures. After Compaq was bought by Hewlett-Packard Co., Lewis was named head of worldwide marketing and solutions at Network Storage Solutions, HP's newest storage division.

Short Takes

VNA Inc. and IBM signed a deal that calls for IBM to supply PCs and servers to Irving, Texas-based VNA's network of 2,500 health care organizations. Terms were announced last week. ... Internet auction company eBay Inc. is buying Mountain View, Calif.-based online payment company PayPal Inc. in a stock-swap deal valued at \$1.8 billion. ... Three security holes in MICROSOFT CORP.'s SQL Server and one in an encryption plug-in made by Network Associates Inc. for Microsoft's Outlook e-mail client were patched by the vendors last week. ... SAP AG issued a warning that it's reducing its revenue and earnings expectations for its just-ended second quarter. ... The U.S. House of Representatives last week approved legislation requiring the NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY to develop standards for improving supply chain integration.

IBM Hits Both Ends Of Storage Market

New Shark servers double performance of predecessor; NAS device aimed at low end

BY LUCAS BEARAN

IBM will soon be offering new low- and high-end storage arrays aimed at challenging rivals such as Hitachi and Dell with faster devices that provide lower ownership costs.

IBM said this week that it will soon release two new ver-

sions of its high-end TotalStorage Enterprise Storage Server, also known as Shark. The new Shark Model 800 and 800 Turbo have, respectively, two and two and a half times the performance of the current model and operate at 2G bit/sec. data transfer rates.

The Shark is available with a

variety of options, including 15,000 RPM disk drives in both 18.2GB and 36.4GB capacities, and is powered by new copper microchips. It also has 64GB of internal cache and 3.2G bit/sec. internal bandwidth.

For greater Royal Ahold NV, the new Shark server "significantly increased the performance" of the company's backup and recovery process and tripled its storage capacity, said Joe Giacometti, senior vice president of IT. Giacometti

also said the new Shark reduced the cost of managing information by \$50 per gigabyte.

The 800 and the 800 Turbo, which carries two additional processors, come with Project eLiza self-management features that enable real-time configuration and management capabilities.

Mike Kahn, president and CEO of The Clipper Group Inc. in Wellesley, Mass., said that with the new Shark models, IBM has caught up with the speed of Hitachi Data Systems Corp.'s Freedom Storage Lightening 9900 enterprise array. "The disks essentially get you the data faster, and these new engines allow you to move it faster," Kahn said.

The 800 will be generally available Aug. 16; pricing will depend on the configuration, which can support RAID-10 data mirroring and striping for performance-sensitive applications, such as online transaction processing and Oracle databases.

IBM last week also announced a pizza-box-size network-attached storage (NAS) device aimed at low and mid-market uses, such as local storage for distributed offices. The TotalStorage NAS 100 array, which has a list price of \$4,420, is the third NAS product IBM has released in the past three years. IBM has used the same software management applications in each. ■

Itanium 2 Adoption Expected to Be Slow

Analysts say OS, software needed to inspire confidence

BY JAIKUMAR VIJAYAN

Intel Corp.'s 64-bit Itanium processors may ultimately replace their RISC counterparts as the technology of choice for high-end commercial server hardware. But don't look for that to happen anytime soon.

The lack of an enterprise-tested 64-bit operating system and applications that can take immediate advantage of Itanium will mean a slow adoption rate, users and analysts said in the wake of last week's introduction of the second-generation Itanium-2 chip.

Intel itself said it doesn't expect differently. "This is not something we expect will ramp up overnight," said Barbara Grimes, an Intel spokeswoman. "We are looking at this as the processor technology for the next 20 years."

Itanium has already begun delivering on some of its promise as a viable alternative to more expensive RISC boxes from vendors such as IBM and Sun Microsystems Inc.

The National Center for Supercomputing Applications

(NCSA) at the University of Illinois at Urbana-Champaign is using Itanium technology to build a Linux cluster with 136 trillion floating-point operations per second for scientific research purposes.

"We've been very pleased with the performance we've seen so far," said Dan Reed, director of NCSA. "It's competitive with what we've seen on ... RISC-based systems."

Big improvement

Based on early benchmarks, Itanium 2 delivers far more power and sophistication than the disappointing first version of the chip introduced in June of last year, analysts said.

"The improvement in performance, at least from benchmark tests, suggests that Intel was listening pretty closely to the concerns and reservations that customers and vendors had to the first-generation product," said Charles King, an analyst at D.H. Brown Associates Inc. in Mountain View, Calif.

But more pieces have to fall into place for users to be able to migrate commercial applications to Itanium with confidence, said Sarang Ghotpande, an analyst at D.H. Brown Associates Inc. in Port Chester, N.Y. The biggest piece needed is

a fully tested, production-ready 64-bit operating system that can take advantage of Itanium hardware, he said. Several operating systems are available for Itanium, including Windows Advanced Server Limited Edition, Windows XP 64-Bit Edition, HP-UX and versions of Linux from Caldera International Inc. and Red Hat Inc. But most of these are really first versions that are unlikely to inspire much confidence among enterprise users, said Ghotpande.

It's the same story on the application software side. Major vendors are porting their software to Itanium 2 — as IBM is doing with DB2 and WebSphere, Oracle Corp. with its 9i database technology, and BEA Systems Inc. with WebLogic. But here, too, the applications are first versions and remain untested on Itanium.

Until the software matures, commercial users are unlikely to use Itanium for anything more than development and testing purposes, especially in a tight economy, King said. ■

HARDWARE COVERAGE

Visit our Hardware Knowledge Center for links to more Computerworld stories.

Circle 14 on Reader Service card

IBM's Faster, Smarter Sharks

Additional software and processors and faster disk drives give the new Sharks:

- 29 bit/sec. data transfer rates
- Two and two and a half times the performance of the current model
- 64GB internal cache and 3.2G bit/sec. internal bandwidth
- RAID-10 data mirroring and striping
- Project eLiza software self-management features
- 15,000 RPM disk drives in 18.2GB and 36.4GB capacities

5 cool things to do while you wait for a disaster to hit your company.

1. Test new applications.
2. Deploy new applications.
3. Shorten backup windows.
4. Refresh data warehouses.
5. Take a whole hour for lunch.

EMC

Business
Applications

Storage
Solutions

Nasdaq Ready to Launch \$107M Stock Trade System

Technology represents bandwidth doubling

BY LUCAS MEARIN

AFTER SPENDING three years and \$107 million on a project that included the installation of more than 200 servers, Nasdaq Stock Market Inc. last week said it's prepared to launch its SuperMontage electronic order display and execution system on July 29.

SuperMontage, which is a real-time, fully integrated order display and execution system, was built in response to issues such as decentralization for the switch-over from reporting prices in fractions on and increased trade volume.

"This should reduce intraday volatility through more information," liquidity "and depth," said Nasdaq President Richard Ketchum.

The backbone of Nasdaq's telecommunications will be managed by WorldCom Inc. and connect 1,000 trade locations across the country to a main data center in Connecticut and a backup site in Maryland. Addressing WorldCom's ongoing financial problems, Nasdaq CIO Steve Randisch said the network is "separate and distinct... and the WorldCom employees are dedicated to the account."

"We're confident WorldCom will be our provider for the next several years," he added.

Test Stocks

Nasdaq plans to open SuperMontage with a few test stocks and then include about 80 additional stocks every week thereafter. Ketchum said he to list New York Stock Exchange securities, but he had no definite timeline for that.

Jim Van Dyke, an analyst at Javelin Strategy and Research Inc. in Pleasanton, Calif., said the adoption of SuperMontage by securities firms shouldn't

be affected by the current economic slowdown. In fact, he noted that rollouts are faster when activity level is low.

Nasdaq's current order display system, SuperSOES, will be used for transactions of fewer than 1 million shares until all securities have transferred to SuperMontage SuperSOES displays the best proposed pur-

chase and selling prices for a stock, as well as who is participating in the market for that stock and each issue's most recent transaction. In contrast, SuperMontage will aggregate the top five proposed purchase and selling prices for a stock, giving traders more access to possible trades and increased transparency, said Aden Friedman, Nasdaq's executive vice president of data products.

"It shows if there are a lot of people interested in buying or selling a particular stock out there," Friedman said.

Randisch said the technology behind SuperMontage represents a doubling of Nasdaq's network bandwidth and offers

Why It's Better

SuperMontage offers improvements over Nasdaq's SelectNet and SuperSOES. For instance, it will:

- Provide a fully integrated order display and execution system.
- Display the top five bids and offers rather than just the single top bid.
- Deliver the information in real time.
- Offer pretrade anonymity.
- Handle more orders, more quickly.

more scalability for adding servers and processors. He said SuperMontage's processing ability is nearing 5,000 transactions per second.

SuperMontage's back-end systems consist of 22 Stratus Computer Corp. Continuum Series 400 servers, 405 Dell servers running Windows 2000 to support new electronic products and surveillance software, and 24 Hewlett-Packard Co. NonStop S86000 servers with 16 processors each. Randisch said Nasdaq will be the first commercial customer to deploy HP's newest high-end server and added that it has performed well in processing performance tests. ■

Continued from page 1

WorldCom

bility issue," said Brannett. "But now it doesn't look like anything is stable."

The WorldCom mess has become a bad dream for many in IT. None of the IT and telecommunications managers interviewed for this article said that they seriously believe that WorldCom's service is going to be switched off, because it's too vital. But they also noted that they have no choice but to

consider "what if" scenarios.

Gary Rosenberg, telecommunications manager at Norwick Inc., a manufacturer of building products in Providence, R.I., relies on WorldCom for voice and data.

Rosenberg is a 42-year telecom veteran, but WorldCom's problems are prompting him to think in new ways. He's talking with vendors about providing a standby service — having lines in place and ready to go if WorldCom fails.

But having seven TI backup lines in just one facility could cost \$100,000 a month, said

Rosenberg. The cost is high because the vendors don't have pricing mechanisms for running lines that aren't also carrying revenue-generating voice and data traffic, he said. Rosenberg counters by telling vendors that providing an affordable standby service could give them a leg up once telecommunications contracts are rebid. Negotiations are continuing, he said.

WorldCom's problems are also a slap in the face to IT managers who review a vendor's financial statements as part of a contracting process. For 15 months, WorldCom allegedly inflated its earnings by nearly \$4 billion.

Due Diligence

Due diligence "just goes out the window if audited financial statements are not to be believed," said Andy Fisk, IT manager at the Tribune Review Publishing Co., a Greensburg, Pa.-based newspaper chain.

Fisk has contracted other carriers to provide backup for his WorldCom services. But like other IT managers, he doesn't want to change providers "on the off chance they [WorldCom] are going to go away," he said. But, Fisk added, "on the other hand, I'd hate to find out that they've gone away and left us high and dry."

One person who has experienced a telecommunications

User Angst

IT MANAGERS ARE CONSIDERING POTENTIAL WORLD.COM FALLOUT:

DIVERSIFICATION

Telecommunications providers price their services to win an enterprise's entire business. The bigger the volume, the lower the cost. But users will likely find having one provider unacceptable.

SHORTER CONTRACTS

One-year contracts are more likely to allow flexibility to respond to pricing changes and provider problems.

COMPETITION WORRIES

If key parts of WorldCom are sold off, competition could emerge, raising prices.

How Ryder Deals With WorldCom

WORLDWIDE WorldCom is a daily topic at Ryder System Inc. The telecommunications company's performance is closely monitored, and once a week a WorldCom official touches base to make sure everything is OK. That's what CIO Eduardo Vial wants.

Ryder, a Miami-based transportation and logistics company with 30,000 employees worldwide and 1,000 locations in North America, is a big WorldCom customer. WorldCom provides close to 80% of Ryder's data and voice services. When WorldCom's problems surfaced, Vial immediately contacted the firm to make arrangements to ensure uninterrupted service delivery. It was

agreed that each week a senior account representative from WorldCom would contact Vial's operations director to discuss systems performance.

WorldCom has "not neglected on providing services that they contracted to us, and I'm comfortable there," Vial said.

Ryder renewed its contract just two months before WorldCom's financial problems were disclosed. But Vial said his company continues to have a good working relationship with the vendor, and he believes that the WorldCom officials he dealt with were unaware of the financial problems. "I have no reason to doubt their honesty," he said.

—Patrick Thibodeau

failure firsthand is Brian Voss, vice president of telecommunications at Indiana University, a 96,000-student institution in Bloomington.

The university was using services from Telelobe Inc. in Reston, Va., when it filed for bankruptcy protection in May Indiana University relied on Telelobe to provide one of two high-speed circuits connecting the university to an Asia-Pacific high-performance research network.

"Our circuit went off," said Voss. "I think what we learned from that experience is that it's probably good to be diversified." ■

Nasdaq Ready to Launch \$107M Stock Trade System

Technology represents bandwidth doubling

BY LUCAS MEERMAN

AFTER SPENDING three years and \$107 million on a project that included the installation of more than 200 servers, Nasdaq Stock Market Inc. last week said it's prepared to launch its SuperMontage electronic order display and execution system on July 29.

SuperMontage, which is a real-time, fully integrated order display and execution system, was built in response to issues such as decentralization (for the switch-over from reporting prices in fractions) and increased trade volume.

"This should reduce intra-day volatility through more information, liquidity and depth," said Nasdaq President Richard Ketchum.

The backbone of Nasdaq's telecommunications will be managed by WorldCom Inc. and connect 1,000 trade locations across the country to a main data center in Connecticut and a backup site in Maryland. Addressing WorldCom's ongoing financial problems, Nasdaq CIO Steve Randich said the network is "separate and distinct..." and the WorldCom employees are dedicated to the account.

"We're confident WorldCom will be our provider for the next several years," he added.

Test Stocks

Nasdaq plans to open SuperMontage with a few test stocks and then include about 10 additional stocks every week thereafter. Ketchum said he is list New York Stock Exchange securities, but he had no definite timeline for that.

Jim Van Dyke, an analyst at Javelin Strategy and Research Inc. in Pleasanton, Calif., said the adoption of SuperMontage by securities firms shouldn't

be affected by the current economic slowdown. To be fair, he noted that rollouts are easier when activity level is low.

Nasdaq's current order display system, SuperSOES, will be used for transactions of fewer than 1 million shares until all securities have transferred to SuperMontage. SuperSOES displays the best proposed purchase and selling prices for a stock, as well as who is participating in the market for that stock and each issue's most recent transaction. In contrast, SuperMontage will aggregate the top five proposed purchase and selling prices for a stock, giving traders more access to possible trades and increased transparency, said Adena Friedman, Nasdaq's executive vice president of data products.

"It shows if there are a lot of people interested in buying or selling a particular stock out there," Friedman said.

Randich said the technology behind SuperMontage represents a doubling of Nasdaq's network bandwidth and offers

Continued from page 1

WorldCom

consider "what if" scenarios. Gary Rosenberg, telecommunications manager at Netek Inc., a manufacturer of building products in Providence, R.I., relies on WorldCom for voice and data.

Rosenberg is a 42-year telecommunications veteran, but WorldCom's problems are prompting him to think in new ways. He's talking with vendors about providing a standby service — having lines in place and ready to go if WorldCom fails. But having seven T1 backup lines in just one facility could cost \$100,000 a month, said

How Ryder Deals With WorldCom

WASHINGTON WorldCom is a daily topic at Ryder System Inc. The telecommunications company's performance is closely monitored, and once a week a WorldCom official touches base to make sure everything is OK. That's what CIO Eduardo Vital wants.

Ryder, a Miami-based transportation and logistics company with 30,000 employees worldwide and 1,000 locations in North America, is a big WorldCom customer. WorldCom provides close to 80% of Ryder's data and voice services. When WorldCom's problems surfaced, Vital immediately contacted the firm to make arrangements to ensure uninterrupted service delivery. It was

agreed that each week a senior executive would meet with WorldCom to discuss Vital's operations director to discuss system performance.

WorldCom has "not neglected on providing services that they contracted to us, and I'm comfortable with that," Vital said.

Ryder renewed its contract just two months before WorldCom's financial problems were disclosed. But Vital said his company continued to have a good working relationship with the vendor, and he believes that the WorldCom officials he dealt with were unaware of the financial problems. "I have no reason to doubt their honesty," he said.

—Patrick Thibodeau

Why It's Better

SuperMontage offers improvements over Nasdaq's SuperSOES and SuperSOES. For instance, it offers:

• Provide a fully integrated order display and execution system.

• Display the top five bids and offers rather than just the single top bid.

• Deliver the information in real time.

• Offer providers anonymity.

• Handle more orders, more quickly.

consider "what if" scenarios. Gary Rosenberg, telecommunications manager at Netek Inc., a manufacturer of building products in Providence, R.I., relies on WorldCom for voice and data. Rosenberg is a 42-year telecommunications veteran, but WorldCom's problems are prompting him to think in new ways. He's talking with vendors about providing a standby service — having lines in place and ready to go if WorldCom fails. But having seven T1 backup lines in just one facility could cost \$100,000 a month, said

WorldCom's problems are also a slap in the face to IT managers who review a vendor's financial statements as part of a contracting process. For 15 months, WorldCom allegedly inflated its earnings by nearly \$4 billion.

Due Diligence

Due diligence "just goes out the window if audited financial statements are out to be believed," said Andy Fisk, IT manager at the Tribune-Review Publishing Co., a Greensburg, Pa.-based newspaper chain.

Fisk has contacted other carriers to provide backup for his WorldCom services. But like other IT managers, he doesn't want to change providers "so the off chance they [WorldCom] are going to go away," he said. But, Fisk added, "on the other hand, I'd hate to find out that they've gone away and left us high and dry."

One person who has experienced a telecommunications

more scalability for adding servers and processors. He said SuperMontage's processing ability is nearing 5,000 transactions per second.

SuperMontage's back-end systems consist of 22 Stratus Computer Corp. Continuum Series 400 servers, 165 Dell servers running Windows 2000 to support new electronic products and surveillance software, and 24 Hewlett-Packard Co. NonStop 586000 servers with 16 processors each. Randich said Nasdaq will be the first commercial customer to deploy HP's newest high-end server and added that it has performed well in processing performance tests. ■



failure firsthand is Brian Voss, vice president of telecommunications at Indiana University, a 96,000-student institution in Bloomington.

The university was using services from Telephone Inc. in Reston, Va., when it filed for bankruptcy protection in May. Indiana University relied on Telephone to provide one of two high-speed circuits connecting the university to an Asia-Pacific high-performance research network.

"Our circuit went off," said Voss. "I think what we learned from that experience is that it's probably good to be diversified." ■

Co-owned
and Produced by
COMPUTERWORLD

STORAGE NETWORKING WORLD

Co-owned
and Endorsed by
SNIA

Storage Networking World® Spring 2002 attendees save solutions from:

PLATINUM SPONSORS



GOLD SPONSORS



CONTRIBUTING SPONSORS



MEDIA SPONSORS



Burger King Upgrades to mySAP.com

Fast-food industry standardizes apps

BY MARC L. BOWMAN

Burger King Corp. is serving an upgrade of SAP AG's business applications to its end users. It's one of a small but growing number of fast-food companies that are standardizing their systems on packaged enterprise resource planning (ERP) applications.

The Miami-based company last month upgraded its installation of SAP's R/3 human resources and finance applications to Version 4.6c. That sets the stage for future phases of the upgrade of Burger King's SAP R/3 ERP application to the mySAP.com suite.

During the next year, the

company also plans to turn on treasury, real estate, budget management and self-service human resources applications as part of the migration, according to Rafael Sanchez, Burger King's CIO.

For Burger King, the big appeal of mySAP is the software's integration capabilities and technical maturation, according to Sanchez.

Between 60% and 70% of the custom modifications in SAP's earlier finance and human resources releases will be replaced by mySAP functionality, he said. In addition, the real estate management application will replace a custom ap-

plication written in SAP's ABAP programming language, Sanchez said.

In general, companies in industries such as fast food and retail have been slower to adopt ERP technology than manufacturers, said Peter Abell, an analyst at Boston-based AMR Research Inc.

Rollout Challenges

Some companies are hesitant to change because they face considerable rollout challenges, especially if their corporate IT systems are linked to individual stores or franchisees that have workers who are relatively unfamiliar with technology, Abell said.

But Burger King isn't alone in turning to a third party.

ERP Drive-through

BURGER KING'S mySAP.COM ROLLOUT PLAN INCLUDES THE FOLLOWING APPLICATIONS:

Live on or last month:
mySAP 4.6c finance and human resources modules

Expected functionality due to be added within the next year:

- Real estate management capabilities
- Treasury management, which handles liquidity, currency issues and investment portfolios
- Self-service human resources tools for use by employees

Chick-fil-A Inc., an Atlanta-based chain, ties its 1,000 restaurants in 34 states to its data center's core ERP system via a virtual private network.

The data center uses Oracle Financials to aggregate sales and daily business data, said Mark Brackett, director of information systems at Chick-fil-A.

Chick-fil-A also plans to add Oracle Internet Expenses to the ERP system within the next month.

Last August, Chick-fil-A upgraded to Oracle's E-Business Suite III from Version 10.7. It installed human resources, financials and payroll applications and added receivables, cash management and order management software.

Brackett said the Oracle suite, which runs on HP-UX servers, has helped Chick-fil-A automate its accounting system, making it possible for the company to open new stores without having to add a commensurate number of IT employees to support them. ■

He Got Past Two Traps, Your Cat,
and the Poison.

How did you know where he was
and what damage he did?

Tripwire Is The Data Integrity Assurance Company

Tripwire® establishes a baseline of data in its known good state, monitors and reports any changes to that baseline, and enables rapid discovery and recovery when an undesired change occurs.

Foundation for Data Security

- Ensure the integrity of your data
- Instant assessment of system state, reporting "integrity drifts"

Maximize System Uptime

- Eliminate risk and uncertainty
- Enable quick restoration to a desired state

Increase Control and Stability

- Ongoing monitoring and reporting

Lower Costs

- Find and fix problems quickly and precisely - no more guess work

Your firewalls and intrusion detection tools alone are not enough to keep systems trustworthy. Tripwire's data integrity assurance products are the only way to know with 100% confidence that your data remains uncompromised. For nearly 10 years Tripwire has been helping IT professionals know exactly what's changed on their systems, and helping them to recover quickly.

For a FREE 30-day fully-functional eval, call toll-free 1.800.TRIPWIRE (874.7947) or visit <http://www.tripwire.com> today!

TRIPWIRE

THE DATA INTEGRITY ASSURANCE COMPANY



FOUNDRY (STRUCTURE). ONE SWITCH FAMILY.
JETCOR (COMPASS) IS YOUR NETWORK ENTER POINT.

JetCor



FOUNDRY
NETWORKS

over a majority of the consumer products giant's back-office operations.

It's this warning shot for a review of IT outsourcing relationships? Outsourcing has been touted as an efficient way for companies to focus on what they do best while palming off the IT drudgery to someone else. But we're learning that the drudgery comes with some high costs and might not be so profitable for third parties without some financial maneuvering.

At the very least, the scandal should refocus the debate on whether IT expertise ought to be a genuine cost, built into the routine of running a business, and whether you can be immunized from the risks of maintaining an IT infrastructure just by signing a contract.

With uncertainty surrounding the accuracy of financial reporting, it's imperative that you know the risks your potential IT outsourcing firms have incurred. Ask who their largest customers are, learn how they plan to account for your business, and check if they're making money from their contracts. That's the only way to verify that win-win is more than a marketing slogan. ■

DAN GILLMOR

Users Must Beware of Legal Trends

THE IT USER community has never thought of itself as making laws, except to the extent of setting down rules inside the enterprise. This is a natural consequence of doing a particular job.

Maybe it's time to think more broadly. The way you do your job is going to have more impact on society at large than you may want to know.

Recently, some top minds in law and technology assembled at the Berkman Center for Internet & Society at Harvard Law School. One was Lawrence Lessig, the Stanford University law professor who said, persuasively, that the future is bleak unless people step up to some serious issues. The forces of absolute control are on the verge of deciding what kind of creativity and innovation will be allowed, and as a result, they're damping down progress.

Lessig's key insight is that code, the zeroes and ones, can become law. IT writes, buys, licenses and uses soft-

ware; code, interrelating with other forces, becomes one of the governing influences on our lives, just as the location of a road changes a community or the absence of a ramp keeps out people in wheelchairs.

Societal norms and the law say you can buy a music recording and make a copy to play in your car. You can buy a book and give it to your child. But in the age of digital content, the owners of the copyrights say these uses are a bug, not a feature.

So they write code that gives them user control over how copyrighted material — or, in some cases, even material in the public domain — may be used. Using code, they forbid those formerly legal and customary uses.

Because the owners are well organized and financed, they have bought



JENNIFER WILLIAMS is a technology entrepreneur at the San Jose Mercury News. Contact her at jwilliams@mercury.com.

If you use open-source software in your business, either because it works well or is a way to keep proprietary software companies from owning you (or both), beware patents. At the Harvard event, a manager of Microsoft's "shared-source" program, in which customers can look at Windows source code under restricted conditions, repeatedly didn't answer when asked if

political support. Recent laws make it illegal to circumvent the code they've used to decimate old law and tradition. And a few big companies, paranoid and stuck with outdated business models, effectively get to determine the parameters of creativity.

The patent system has also run amok. Software and business-process patents are a clear and present threat to innovation.

is "genuine." The benefits to consumers, if any, will be inconsequential. The true beneficiaries will be groups that desire to limit the way we use our computers. I used to think Microsoft was the best, but my freedom to use what I purchase in the way that I want without permission or activation is more important than jumping on the bandwagon and supporting the only game in town.

Vic Russell
IT spacer
Hertie Group Building Dept.
Medina, Ohio

ALTHOUGH the plans for Palladium sound like an improvement for security, I wouldn't want any hardware modifications that would lock the info Windows and out of, say, Linux.

Roy Hooper
Durham, N.C.

Open Source Is Imperfect

NICHOLAS PETERLEY'S column "Open Source's Open Door" [QuickLink: 30647] fails to recognize several facts. First, if a vendor changes source code to correct a security hole, it's responsible for any problems created by that change. Second, in-house modification requires considerable resources to maintain and document code changes.

Third, while open source isn't attacked as often as Microsoft systems, that will change when it becomes as common as Microsoft products. Finally, open source's very nature provides an open door for those seeking to exploit its weaknesses.

Alan Marger
Baltimore

Palladium Locks Windows

DO YOU TRULY believe Microsoft is pushing Palladium for user security [QuickLink: 30609]? Absolutely not. It wants to be sure that every machine can run only Windows and that every copy of Windows

Must There Be Only One?

MARK HALL's editorial, "The Real Trial," in which he says Microsoft's influence will inevitably diminish regardless of the outcome of its an-

titrust trial, was well put [QuickLink: 30951]. Have you noticed how the power is returning to — ahem — IBM? I guess it never went away after all. Is there something about computing that insists there be only one dominant player?

Steven Rubenstein
Marlborough, Tenn.

Spam Blocked, for Free

ONLY ENOUGH, the most effective spam blockers are free [QuickLink: 30604]. Use Sendmail as your mail server software and add a DNS-BL (DNS blocking list) to your feature list. Spamcop, SPEWS, ORDB and others all cost nothing, and they all block most spam. I know — I use them on the mail server of my nonprofit client, and my ISP uses some set of them on the mail server that I get my regular e-mail through. I average less than one spam per day, and since I forward those spams to Spamcop to improve the filter, they don't evade the filters for long. So far, a review of our reject lists shows only minimal false positives.

Microsoft intoned, as a senior executive has openly threatened, to use its growing patent portfolio against open-source programmers.

IT needs to consider its own needs and consequences. Many of you are telling Microsoft you want locked-down PCs — far more so than today's models — that can do only what systems administrators allow them to do. This, after all, can ensure adherence to corporate information policies and, perhaps, boost security.

Bake this into the operating system, and you've solved one problem. But you've helped spawn a new monster, a regime in which Microsoft and its new allies in Hollywood and government become arbiters of far more than they already control today.

It's a world where end users — and technology innovators, including IT — will need permission to do what's already legal and critical to lives and businesses. Is that what you want? ■

(Sources of legitimate mail.)

Charles Ornt
National legislative chair
Association of Information
Technology Professionals
Littleton, Colo.

Can't Plan for Fashion

WHILE THERE ARE certainly benefits to be had using

CPFR, I think this is true only for products that are fairly stable in nature, such as toothpaste and laundry soap [QuickLink: 30996]. With the fickleness of fashion, apparel retailers would only be guessing.

Bob Felony
Van Nuys, Calif.
rfelony@msdprg.com

COMPUTERWORLD welcomes comments from its readers. Letters will be edited for brevity and clarity. They should be addressed to: **Jane Eickel**, letters editor, Computerworld, PO Box 977, 500 Old Connecticut Path, Framingham, Mass. 01701. Fax: (508) 678-4843. Internet: letters@computerworld.com. Include an address and phone number for immediate verification.

For more current letters on issues and other topics, go online to computerworld.com/letters

**"Cable & Wireless...
Most financially
stable operator
in class."**

— CommunicationsWeek International, Network Top 500 Survey 1999

Reliability extends far beyond the network.

When it comes to Internet services for your business, the financial stability of your provider is vital. Cable & Wireless is ranked the "Most financially stable operator in class" by CommunicationsWeek International. Our wholly owned, tier 1 global IP backbone spans six continents and 50 countries. We offer a full suite of Internet services – from dedicated access to a flexible portfolio of managed hosting solutions. With a balance sheet that says we'll be here tomorrow, we're setting the standards for reliability, performance and service. Find out more at www.cw.com/reliable or call 1-866-598-0799. It's a solid investment.



EDITOR'S NOTE

MY COLLEAGUE Frank Hayes says that "security is the new Y2K" (QuickLink: 80719). And he's right: IT security is in a state of crisis on both the vendor and user sides and needs a full-scale remediation effort.

But security doesn't have the immovable deadline that was so good at focusing everyone's attention on the Y2K problem and breaking through the usual logjams. Lacking a natural deadline, maybe the pressure for remediation will come from security audits by the federal government, as predicted by futurist Thornton May (page 47).

Short of federal audits, the pressure will have to come from corporate CEOs. Unfortunately, like Y2K, security doesn't have a clear-cut ROL. So, how are we going to get the CEO's financial support for major investments in IT security and disaster recovery? I suggest asking your CEO three simple questions:

• How will the board react if Russian hackers steal \$10 million from our accounts? (It happened to Citibank in 1994.)

• How will we stay in business if employees can't get into the headquarters building because it's been cordoned off due to an anthrax scare?

• How will it look on Wall Street if we're hit with a "security malpractice" lawsuit because we failed to close security holes that were widely known?

For starters, let's do the easy stuff. GarnerG2 predicts that 90% of cyberattacks will exploit known security flaws for which a patch is available or a solution known. That's why one of the tasks on the to-do list in this special report is patch management (page 28). We also suggest assembling a SWAT team to handle security incidents and distributing IT resources for better disaster recovery.

We can help set the agenda and provide implementation tips, but you'll have to get the CEO to open his checkbook yourself. ■

Mitch Betts (mitch_betts@computerworld.com) is director of Computerworld's Knowledge Centers.

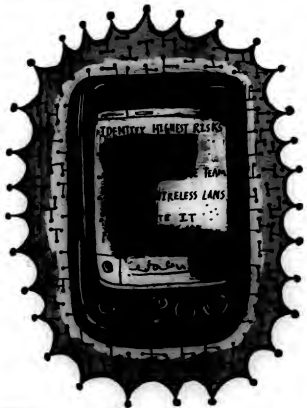
KNOWLEDGE CENTERS ONLINE

Knowledge Centers provide practical information about specific IT topics. In addition to this monthly Special Report in print, there are numerous resources at our Web site, including research links, glossaries, white papers and the following online features:

Industry Q&A: Reserve Mitchell Sandler of IBM Global Services discusses the hot trends in corporate security and disaster recovery.

Case Studies: Companies tackle issues such as disaster recovery for laptops and how to monitor all those security sensors.

QuickLink: 81800
www.computerworld.com



The Security Action Plan

SPECIAL REPORT

Here's a to-do list that ranges from managing patches to securing wireless LANs.

on the road

VPN/SECURITY

IP COMMUNICATIONS

CONTENT NETWORKING

OPTICAL NETWORKING

STORAGE NETWORKING

cisco.com/go/mobility

tools, and information databases while on the road, at home or at work. With Cisco AVVID enterprise architecture, you can do all this without any disruption. This standardized enterprise architecture allows you to seamlessly integrate wireless, voice, video, and data applications on a single, scalable network. This includes new and existing technologies alike. Whether you're building your enterprise network or extending it with Cisco Powered Network services, take advantage of the tools below to get it done right.

CISCO SYSTEMS



EMPOWERING THE
ENTERPRISE GENERATION



GOING MOBILE, STAYING SECURE

BUSINESS RESILIENCE IS REINFORCED WHEN USERS CAN
SECURELY CONNECT FROM WHEREVER THEY ARE

How can enterprises remain productive and competitive in the face of changing—and often unpredictable—business conditions?

This question is on the minds of many IT managers today. One reason is that businesses worldwide witnessed unprecedented economic changes and disasters this past year. As a result, IT departments are building extra measures of business resilience into their computing, application, and network infrastructures.

Today, enterprises are discovering that in addition to mirrored data centers and network backup systems, mobility is becoming a key component of business resilience. Empowering users to remain productive whenever they are located keeps businesses agile and competitive as they decentralize their operations and scatter employees among headquarters, branch offices, and home offices, and while users spend increasing amounts of time away from the office on business travel.

"If users do not have access to all their productivity tools when they are away from their desks, this is a missed opportunity to push a business forward," says Charlie Giancarlo, senior vice president of technology development at Cisco Systems. Cisco helps businesses address this challenge with the Cisco Mobile Office, a set of solutions that empowers IT departments to provide secure, high-speed connectivity to mobile users.

One example of mobility as it relates to business resilience is the impact that new security regulations in the airline industry have had on the traveling public. Business travelers now find themselves with significantly more "down" time in airports. If equipped with wireless LAN

client adapters and secure virtual private network (VPN) client software in their portable computers, these users have the ability to leverage emerging public wireless LAN services to remain productive. In addition, hotels and conference centers are also offering both wireless and wired Ethernet services for connecting mobile users to their corporate resources via the Internet.

"Similarly, if a natural disaster or weather conditions prevent employees from getting to a physical workplace, users who can connect securely from home can also keep the business moving without much interruption," says Giancarlo.

THE THREE FLAVORS OF MOBILITY

Users become mobile when they leave their wired LAN connections and roam elsewhere with their laptops and handheld data devices. From there, they might switch to a wireless LAN connection as they join a meeting down the hall or work from an airport. Or they might plug into another wired broadband connection from home or a hotel that offers wired Ethernet services.

Through the Cisco Mobile Office, Cisco offers the networking tools that enable IT managers to support these different types of connections. With these liberating capabilities, though, emerge fresh security challenges, particularly in the wireless sector. Successfully addressing security is critical to maintaining business resilience.

Here, we'll examine how the Cisco Mobile Office enables both wireless and wired mobility for business customers while solving the security challenges associated with them.

Cisco Systems



COMPUTERWORLD
CUSTOM PUBLISHING

AT WORK: WIRELESS LANs

The Cisco solution for mobility within the enterprise centers around the Cisco Aironet® wireless LAN system, which includes the Cisco Aironet 1200 Series dual mode access points for both IEEE 802.11b (11 Mbps) and 802.11a (54 Mbps) networking, client adapter cards, and the Cisco Access Control Server for authentication.

Wireless LANs deliver the freedom to work virtually anywhere within a building or around a corporate campus without the limitation of wires or cables. People in a conference room can access information needed to make decisions, for example, rendering meetings more productive. Moreover, wireless networks can serve as a cabling replacement to overcome business limitations created by older buildings and temporary work areas.

Evidence of the potential impact of wireless LANs on user productivity was revealed by a study conducted last fall by NOP World - Technology, a research company that surveyed more than 300 U.S.-based organizations with 100 or more employees using wireless LANs. The study showed that wireless LAN technology allowed users to stay connected for an additional 1.75 hours each day, which increased their productivity as much as 22%.

SECURITY AT WORK

Despite the significant productivity enhancing potential of wireless LANs, many enterprises have been hesitant to fully embrace them, largely because of security concerns. These worries were fueled by reports last year that the basic security algorithm in the IEEE 802.11b wireless LAN standard is easy to crack.

These vulnerabilities have since been overcome by the security enhancements in Cisco Aironet products. The Cisco Wireless Security Suite, which includes reinforced encryption and authentication, makes it possible for IT departments to unenthrall users without sacrificing network security.

Sharp Healthcare, a regional healthcare delivery system based in San Diego, California, for example, uses Cisco Aironet wireless LANs to improve patient care by enabling bedside care givers to access patient data records, order lab tests, and issue pharmaceutical prescriptions. Without the Cisco Aironet



enhanced security measures, Sharp would be hard pressed to meet the stricter standards for patient confidentiality recently mandated by the Health Insurance Portability and Accountability Act (HIPAA), comments Mark Weisenberg, Sharp's director of network services.

"The HIPAA requirements have a direct bearing on wireless data transfer, and we need absolute certainty that we were not going to put patient records in jeopardy with our wireless system," he says.

What are the security risks associated with wireless net-

works? In general, enterprises must protect themselves from unauthorized individuals gaining access to corporate servers or "stealing" data in transit. They also need to guard against denial of service attacks on corporate Web servers, which clog them up with bogus service requests and prevent user and customer access to data and services.

These vulnerabilities exist in wired networks, too, but wireless LANs open an additional exposure that must be addressed specifically, because radio signals can penetrate walls. If the proper security mechanisms are not in place, someone outside a building but within range of an access point could circumvent the firewall and hop onto the enterprise network.

Today, enterprises using wireless LANs have deployed four distinct forms of security: open access (no security), basic security, enhanced security, and specialized security. The primary reason some enterprise installations have no security is that, in accordance with IEEE 802.11b specifications, systems ship by default with basic encryption disabled, and companies are not turning it on. Even when these features—called Wired Equivalent Privacy (WEP)—are activated, though, the static nature of the WEP encryption key still leaves companies at risk. Static encryption keys rarely change, leaving hackers plenty of time to decode them.

The Cisco Wireless Security Suite enables both enhanced and specialized security to overcome static WEP vulnerabilities for enterprise-class protection. Within the enterprise, enhanced security is recommended, while specialized security in the form of a VPN based on the IP Security (IPSec) standard is appropriate for users on the road.

For enhanced security within the enterprise, Cisco

has expanded the industry-standard Extensible Authentication Protocol (EAP), which fits into the IEEE 802.1x standard authentication framework, to create an authentication algorithm called EAP Cisco Wireless (also called "Cisco LEAP"), which enables per-user, per-session authentication. Cisco products also support dynamic encryption keys and a pre-standard version of Temporal Key Integrity Protocol (TKIP), which adds per-packet keying, fast rekeying, and message integrity checks to 802.11 security. Together, these capabilities make sessions nearly impossible to hack.

To guard against wireless-initiated denial-of-service attacks, EAP Cisco Wireless supports mutual authentication. "In addition to the user being authenticated, the access point to which the client is connecting must also be authenticated," explains Feyman Roshan, Cisco technical marketing engineer. "This prevents unauthorized access points from being set up inside buildings, from which someone could launch denial-of-service attacks onto a corporate Web server."

ON THE ROAD: PUBLIC LAN SERVICES

Users who spend a substantial amount of time on the road have an increasing array of connectivity options. As mentioned, the availability of wireless LAN services for high bandwidth access to the Internet is proliferating in airports, convention centers, public hotel areas, restaurants, and coffee shops. Wired Ethernet connections are also becoming available in hotel rooms and other locations.

The property owners and service providers supplying these services to enterprise users can deploy them using infrastructure equipment made by Cisco. For example, hotels can run Cisco switches that support Cisco Long Reach Ethernet technology to support multimegabit-speed connections in guest rooms wired with older Category 12/3 telephone wiring. Similarly, Cisco wireless access points can be installed in public venues to enable open access wireless LAN connectivity to the Internet.

All traveling business users need to use these services are the appropriate client adapters in their portable computers to access these wired or wireless networks. As mentioned, VPN client software is also highly recommended for security.

What about handheld devices? Presenting content on small displays necessitates a transformation function to reformat the HTML and XML content residing in corporate Web servers that has been tuned to

desktop-sized displays. In addition to performing markup language translation (such as HTML to WML), it is important to deliver the right subset of data to the requesting device. The Cisco CTE 1400 Series Content Transformation Engine, for example, front ends an organization's Web servers to transform content for display by a variety of mobile devices using default or customized rules.

SECURITY ON THE ROAD

When users connect to their corporate networks from the road, IPsec VPNs protect against hack attacks on remote access connections. IPsec VPNs have two components: client software that resides in the user's mobile computer and a security gateway at the corporate site, such as the Cisco VPN 3000 Concentrator. Encrypted tunnels run between the client and the gateway, which terminates the tunnels and decrypts data.

For public wireless LAN services, IPsec VPNs are especially encouraged. Access points in these loca-



tions generally run with their vendor-specific security mechanisms disabled to encourage open access to all potential users. Since the radio signal does not have any physical security associated with it, strong encryption in the wireless access network, supplied by the client VPN software, prevents hackers from stealing data out of the air.

AT HOME: BROADBAND ACCESS

The mobility component of business resilience includes corporate teleworking programs, which let employees work productively from home. According to a 2000 survey by Kinetic Workplace, U.S. companies with teleworking programs saved approximately \$12,000 a year per teleworker and also reduced real-

estate costs as much as 60%.

Workers at home require secure, high-speed connections to their corporate networks. Sometimes the access services available in the various employee locations differ, so a company might need to support a mix of ISDN, DSL, cable modem and other broadband connections.

Cisco has a variety of broadband access products for at home workers. For example, the Cisco 806 Broadband Gateway Router connects to any type of high speed access connection through an Ethernet WAN port. So while an organization may not be able to standardize on the type of broadband network service used by its teleworkers, it can standardize on a single equipment platform.

SECURITY AT HOME

IPSec VPNs again come into play for securing connections from the user's home site across the untrusted public Internet to the corporate VPN gateway. There are several equipment options for teleworker security; the choice often depends on the equipment available from the service provider.

The Cisco 837 Router, for example, has built-in security, including stateful-inspection firewall capabilities and VPN support with IPSec 3DES encryption. There are other security options as

well, including the Cisco PIX 501 Firewall and the VPN 3002 Hardware Client. To ease the administration of corporate teleworking programs, central IT staff can use special software that distributes predefined security policies out to large numbers of Cisco 800 Series routers and security appliances.

EMPOWERING THE ENTERPRISE WITH MOBILITY

Because of the enhanced capabilities now available for securing connections across untrusted wireless networks and the public Internet, enterprises can embrace mobility as a key component of their business resilience strategies. This empowers companies to keep business processes going when users are away from a traditional office workspace with a wired connection to the corporate network. Employees who can get connected both within and outside of the corporate walls are employees who stay productive and, as a result, increase their companies' competitive power.

FOR MORE INFORMATION

SECURE ENTERPRISE MOBILITY SOLUTIONS FROM CISCO

Mobility Application	Product	Description
At Work	Cisco Aironet 1200 Series Access Point	Dual-mode 802.11a/802.11b radio that provides wireless access to the corporate network
	Cisco Aironet Client Adapter Card	Wireless LAN interface card that secures connections using the Cisco Wireless Security Suite
	Cisco Access Control Server	A RADIUS authentication server that supports Cisco LEAP security protocols
On the Road	Cisco IPSec VPN Client Software and VPN 3000 Concentrator	Together, establish secure "tunnels" for remote access using DES or 3DES encryption algorithms
	Cisco Aironet Client Adapter Card	Wireless LAN interface card. When used with public network services, security is achieved using specialized IPSec VPN technology (see above).
	Cisco CTE 1400 Series Content Transformation Engine	Dynamically transforms Web content so that it is properly displayed on the small screens of handheld devices
At Home	Cisco 800 Series Routers	Connect users to broadband Internet services for access to corporate resources. Some support integrated stateful firewall and IPSec capabilities.
	Cisco PIX 501 Firewall	Security appliance that provides up to 10 Mbps of firewall throughput and 3 Mbps of 3DES throughput
	Cisco VPN 3002 Hardware Client	Provides secure connections to a VPN 3000 Concentrator at a central site using IPSec tunnels

A LOCK ON THE DOOR was state-of-the-art security for data centers 40 years ago. Programs were run in batch mode with no remote terminals, so the greatest risk to data security was that a mainframe printout might be retrieved from a trash bin. And disaster recovery largely consisted of making sure that, should there be a power outage, reels of tape were carefully removed from tape drives; the tapes could be damaged if the power suddenly came back on.

That was the last time security would be so simple.

By November 1968, developers at MIT were demonstrating their experimental Compatible Time-Sharing System, which allowed four users working at terminals to run programs at the same time. Time-sharing meant users could intentionally interfere with other users' programs — and by the late 1960s, terminals connected by modem meant that an outsider could learn a password and log in. But there was little risk of that at first, since a remote terminal cost as much as a new car.

Mainframes and minicomputers offered little protection against malicious behavior by internal users. Prank programs that created copies of themselves on a computer until it crashed, and "trapdoor" codes that gave one user access to another's work, were in use by 1972. The first desktop computers hit the market in 1975, and, along with rapidly falling prices for modems, they helped set the stage for what would later

The Story So Far

IT copes with trapdoors, worms, Russian hackers and Hurricane Hugo. By Frank Hayes

become an epidemic of hacking aimed at corporate systems.

Encryption was the way to protect data from prying eyes as it moved through modems or networks. In 1976, the U.S. government officially approved its Data Encryption Standard (DES), which became widely used for financial information sent electronically. That same year, three researchers — Ronald Rivest, Adi Shamir and Leonard Adleman — developed a practical version of public-key encryption,

which had been invented in 1976 by Whitfield Diffie and Martin Hellman as a way to easily encrypt communications of all kinds.

But encryption wouldn't solve all security problems. In 1982, the first computer virus was infecting Apple II computers. IBM PCs had viruses of their own by 1986; commercial antivirus software was available by 1988. And hostile hackers learned to use the Internet. In 1986, astronomer Clifford Stoll tracked down a 75-cent accounting discrepancy and helped catch five German hackers who had broken into 450 computers. Other hacker hunters were at work too — but there were far more hackers.

Preparing for Disaster

The Internet had problems of its own. On Nov. 2, 1988, Cornell University student Robert Morris released a "worm" program onto the Internet that infected 6,000 host computers — 10%

of all Internet hosts — and crippled the Net for days.

Meanwhile, disaster recovery had come into its own. By 1980, Comdisco Inc. and other companies had begun providing disaster recovery services. By the end of the decade, more than 40% of businesses had disaster recovery plans. And they needed them, what with Hurricane Hugo and the San Francisco earthquake in 1989, flooding of underground tunnels in Chicago and Hurricane Andrew in 1992, the bombing of New York's World Trade Center in 1993, and another big quake in Los Angeles in 1994, along with a steady stream of smaller catastrophes that threatened ever more business-critical IT shops.

Mother Nature wasn't the only threat, as some hackers became ambitious cybercrooks. In 1994, a group of Russian hackers siphoned \$50 million from customer accounts at Citibank; they were caught the next year. Other hackers attacked Internet businesses to steal credit card and Social Security numbers.

Encryption was under attack too — by its supporters. In June 1997, a project called Deschall linked tens of thousands of computers on the Internet to crack the 20-year-old DES algorithm in 96 days. Less than a year later, the Electronic Frontier Foundation used a custom, \$250,000 computer to crack DES in only 56 hours. The U.S. government began to relax restrictions on exporting stronger encryption systems and officially approved its Advanced Encryption Standard in May 2002.

In the aftermath of the Sept. 11 attacks, security is a bigger issue for IT than ever before, with new efforts to protect systems and close software holes — and use technology to track down terrorists.

And now, on with the story... ▶



1986: Cars try to leave New York during the Northeast blackout, the first major regional disaster affecting corporate data centers.

1982: First computer virus in the wild infects Apple II computers.

1996: Phil Zimmermann releases his free Pretty Good Privacy public-key encryption system.

1997: DES encryption is cracked in 96 days.

1976: Whitfield Diffie and Martin Hellman invent public-key cryptography.

1980: Comdisco gets into the disaster recovery business.

1988: Software vendors offer first antivirus products.

1988: Robert Morris releases his "worm" program, which infects 10% of the Internet and cripples it for days.

1994: Russian hackers steal \$70 million from Citibank accounts.

2000: First denial-of-service attacks cripple Web servers.



Six steps to cutting costs and counting savings.

By Deborah Radcliff

ROI

LIKE A LOT of other security professionals these days, Mike Hager, security chief at Oppenheimer Funds Distributor Inc. in New York, is under excruciating pressure to provide top-notch protection of data, ensure privacy and manage user access — all on a drum-tight budget. He also needs to justify all project costs and results to top management.

Knowing this, Hager says he doesn't try to sell a security project unless he can first explain its value in terms the business side understands. The best method is to show a reduced cost of administering security, which IT managers say is the only way to demonstrate return on security spending.

"Show me the money" is something of a new commandment for security professionals long accustomed to concerning themselves more with passwords than with payback projections. But fortunately, there are proven steps that security managers can take to get their networks and systems ready for

future security investments that could yield a positive return. There's also a spate of new products aimed at reducing security overhead costs. Using the two together, there's hope for beleaguered security professionals seeking to quantify the positive results of their work and show where and how it adds value to the business.

1 **Know your business.** "You can get value from security programs if you map your technical measures to your business needs," says Steve Hunt, an analyst at Giga Information Group Inc. in Cambridge, Mass. But, he adds, "unfortunately, over 30% of all IT security spending is poorly focused and ineffective by best-practices criteria."

Mail servers are a prime example, Hunt says. "If the mail server goes down, the response team goes to Defcon 5, the highest and most expensive security response," he explains. "But in many cases, the business manager says 'Ho-hum, maybe now I can get some real work done.'"

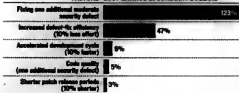
The lesson: Know what's critical to the business and adjust security accordingly. "If you've got systems that are really critical to a business process, [and] you know where your most proprietary secrets are, then you know where to prioritize [security] money and allocations," says Charles Neal, vice president of managed security services at Exodus, a Cable & Wireless Internet Services Inc. company in New York. "For other systems, it may not be a catastrophe if someone broke in, so you spend less."

Maximum Security

Sensitivity Analysis

ROI increases when security is designed into systems, rather than added later.

FACTORS COST SAVINGS IN CONSTANT DOLLARS



SOURCE: METAWARE INC., CAMBRIDGE, MASS.

2 **Form alliances.** Locating risk-sensitive data and systems also means building alliances with business managers. Motorola Inc. in Schaumburg, Ill., does this by placing an IT security officer in each of the company's six business units to represent the business requirements to the IT team and vice versa.

"The job of our business unit security officers is to adapt, refine and deal with the implications that support the critical priorities of the business, while following our corporate policies and standards for enterprise-level technologies," says Chief Information Security Officer Bill Boni.

3 **Set standards.** By blending business requirements with best practices, the security team can establish rules-based security standards for operating systems and platforms. This way, IT organizations can better target security spending, including training dollars, for secure systems administration, says Boni.

These operational standards should include specific instructions for where and what to patch, which services to disable or leave on, which operating sys-

tems to harden, which types of systems to allow on the network, and where to implement additional security capabilities, such as row-level encryption or public-key infrastructure.

Standards-setting is especially important in mergers. "We're taking the best of policies and standards for each company and coming up with new policies, and then setting operational security standards as part of the auto-build procedures for each new system that gets deployed," says Pat Hynes, manager of corporate information security engineering at Wachovia Corp., a Charlotte, N.C.-based financial services firm that merged with First Union Corp. in September.

4 **Bake-in security.** Standardizing security rules can reduce the cost of providing secure configurations to other IT departments. Hynes notes, because it requires IT groups to "bake-in security in products and processes at the onset, rather than repair after the fact."

In May, the Hoover Project, a research arm of @Stake Inc., a Cambridge, Mass.-based security company, released the results of a quantitative study that rated the cost savings of pre-engineered

security against postdeployment security repairs. Forty-five homegrown and commercial applications were tested (see charts). "If you build in security during the design phase of your applications, you can reduce your risk by 80% and achieve rework savings of 28%," says Andrew Jaquith, Hoover's program director.

5 **Assess, benchmark, and then count the savings.** Knowing whether established standards are being met is where the process can become more technical. Consider Motorola's ambitious goal of aligning standard build features with audit compliance. Boni is automating this task with the help of a vulnerability scanning tool called FoundScan from Foundstone Inc. in Mission Viejo, Calif. Like many assessment tools, FoundScan reports on the state of security throughout the network and sends alerts when something falls out of specification.

For benchmarking, the best type of assessment products or services would be those that adapt to the corporation's own security standards, send notification when corporate policy has been violated and provide audit reports that can be used to show security effectiveness. Corporate boards and regulators are beginning to require all three, according to Michael Reszler, director of security services at Predictive Systems

Inc., a network security consulting company in New York.

Since assessing the network manually with internal staff is financially prohibitive, the products are easily justifiable. For example, John Shields, senior vice president of e-business at Pateco Credit Union in San Francisco, says IP540, a tool from eCircle Network Security Inc. in San Francisco, costs him \$50,000 per year. That's \$100,000 less than he would have spent on the manpower to do the same tasks. And Motorola is paying tens of thousands of dollars per year instead of millions for its perimeter assessments alone, says Boni.

But technology doesn't fully gauge the effectiveness of policies as they pertain to people and processes. For this reason, Giga has launched an assessment service called the Security Action ReportCard, which is suitable only for large organizations. The Giga service goes beyond technical assessment programs to assess people and processes, compare them to industry best practices, and map security measures to business requirements to help achieve better cost-effectiveness.

6 **Don't go it alone.** There are many other vendor services available to market to help IT managers reduce administrative overhead for current security processes. For example, managed security services provided by outsourcees are saving some midsize companies up to 80% of what it would cost to monitor security events in-house. New forms of middleware are also springing up to consolidate security report information from intrusion-detection, antivirus and firewall sensors to offer better response and correlation. And larger vendors, such as Cupertino, Calif.-based Symantec Corp., are cobbling together suites with central management interfaces.

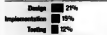
The bottom line: "The reality in business is budget," says Gartner Inc. analyst John Pescatore. And that goes for security as well.

"Security has to be the company make more money by supporting business processes, instead of just preventing bad things that could happen," Pescatore says. "So good security officers usually have good security organizations, even if they're spending less than industry average." ▀

Measuring ROI

Costs savings increase the earlier security is addressed in the development cycle.

PHASE COST SAVINGS



SOURCE: METAWARE INC., CAMBRIDGE, MASS.

Returns

BANG FOR YOUR BUCK

Visit our Web site for tips to cut your security costs and a list of additional online resources.

QuickLink 01241

www.computerworld.com

Manage Those Patches!

Software makes fixes easier, but identifying what needs patching is still a costly hassle. By Stacy Collett

EVERY MORNING, Mark Bialik diligently scans 30 to 40 vendor and security Web sites looking for the latest patches for Infinity HealthCare's many Microsoft Office, Web server and Windows NT-based applications.

On a good day, it takes two hours to conclude that no new patches have been issued. On a not-so-good day, Bialik spends up to four hours figuring out if he's running the affected software. In the worst case, such as when the Code Red worm hit last July, Bialik's day is consumed by installing patches for 20 servers and hundreds of PCs. "I remember a time when I spent three to four days straight doing nothing but patches," says Bialik, a network and security manager at the Mequon, Wis.-based health care provider.

These days, new security software makes it easier to distribute and test patches. But finding a fast and reliable way to identify new patches and prioritize installation remains elusive and costly.

Companies spend more than \$2 billion annually on patch research and deployment, according to Aberdeen Group Inc. in Boston. Meanwhile, the pressure to find and install every patch is increasing as companies heighten security and focus on intrusion detection and managed vulnerability scanning.

It has to be done, so how can systems administrators and security managers make patch management more manageable? Security software vendors, end users and analysts offer the following three tips:

1 Develop a "Patch Network"

Security software products can help streamline the process of finding patches by offering links to vendor sites. But vendors have come under scrutiny for not releasing patches fast enough for their users. Problems and patches can be more quickly identified by establishing a network of peers in multiple organizations, such as former colleagues or people at like-minded institutions, says Eric Hemmendinger, an Aberdeen Group analyst. "They may be your best resource," he adds.

Security portals such as Sens.org and Incidents.org also provide a front line for identifying patches and fixes. "Find good, reliable places that gather the data for you, and make a habit of reading them daily," Bialik says.

2 Buy Time by Prioritizing

Before rushing to install every patch that comes along, prioritize installations according to their impact on the organization.

A vulnerability in an e-commerce application should take priority over one in a platform that's fairly well hidden from the Internet, for instance.

If a high-priority vulnerability is identified, security managers are finding that multilayered security software, which is located at the firewall as well as

Do's and Don'ts

DO establish a network of peers outside your organization to help identify vulnerabilities and find patches.

DO prioritize installations according to their impact on your organization.

DO invest in security software that keeps a log of patches installed on each PC and server.

DON'T rely on quick fixes offered at hackers' sites.

DON'T install patches without first testing them in a development environment.

the lowest level of the network stack, can temporarily plug the hole until a permanent patch is installed.

"Customers recognized this benefit before we did," acknowledges Jon Greene, senior vice president at Network-I Security Solutions Inc. in Waltham, Mass., which sells a line of software security products. "If the intrusion can be detected, we can identify it and stop it. That buys them time to assess the appropriate patches that need to be deployed."

No matter how critical the patch may be, don't rely on fixes offered at hackers' Web sites; they can't be trusted, Bialik offers this advice instead: "If you can get by without running that particular application for the time being until the fix is out, turn it off!"

3 Evaluate Before You Patch

To save yourself time and legwork, invest in security software that keeps a log of patches installed on each PC and server.

The software can also check to make sure patches are working and will rank the vulnerability of each application.

Klipsch Audio Technologies uses San Diego-based St. Bernard Software Inc.'s Update Expert to identify servers and PCs that need patches, scheduling upgrades after business hours. "Something that would've taken six people four hours to do, we can set up in 10 minutes and not have to worry about it," says Mike Fulton, a network manager at the Indianapolis-based audio systems manufacturer.

Another tip: Test the patch first in a development environment to make sure it won't create new problems with the rest of the system. Companies that don't have the luxury of a complete test environment can develop a scaled-down version with at least a copy of the operating system running the applications in production.

And finally, beware of the pitfalls of patch-management software. Users report confusion over which security patch service packs work with different software versions. They also tell of technical support staffers who refused to help with a patch because their companies weren't running the latest version of the vendor's software. Other users say some scanning software can give false positives on uninfected machines. ■

VENDOR PATCHWORK

When it comes to a complete product for patch management, no single vendor meets all the needs of most IT buyers.

QuickLink: 00010
www.computerworld.com

Collett is a freelance writer in Sterling, Va.

The
“WE LEAD THE PACK IN
**CLUSTERING
TECHNOLOGY**”

storage software company.

VERITAS

INTEGRATION IS ONCE AGAIN A POLITICAL ISSUE.

USA PATRIOT ACT

United States Congress

SYBASE e-BUSINESS SOFTWARE. EVERYTHING WORKS

THE STRAIGHT GOODS ON SOFTWARE INTEGRATION.

The USA PATRIOT Act now presents everyone with an enormous information integration challenge. The experts agree that manual review processes for your customers and their financial transactions will no longer suffice. Non-compliance is not an option. The only question facing you is: should you engage as your partner in implementing a solution?



THE SYBASE APPROACH

Our approach leverages the knowledge and capabilities we've developed over nearly 20 years of managing information, application and process integration.

The Sybase PATRIOTCompliance Solution helps you satisfy the integration requirements of the USA PATRIOT Act by implementing a totally automated process for filtering your customers, employees and suppliers against known suspects, and for continuously monitoring their activities. Our solution is operationally unobtrusive, secure and cost-effective.

THE FIRST STEP

Our first step is a Business Requirements Assessment that helps determine your organization's unique needs.

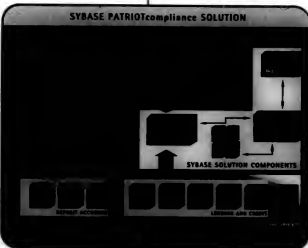
We work with you to understand your front and back office infrastructure. We embrace the technologies and product standardization of your environment. We extend the Anti-

Money Laundering and Bank Secrecy Act investments you've already made. We make our solution work for your people.

Having tuned our PATRIOTCompliance Solution to your environment, we implement, rigorously test (to the very exacting standards we developed to earn ISO 9001/TickIT Certification) and deploy the solution.

and an array of adapters (F.I.X., SWIFT, Flat Files, database, CICS, and others) for accessing and presenting demographic and transaction information from your core systems.

BPI Suite is a comprehensive set of tools to enable you to rapidly build, manage, monitor and improve complex business processes. It also speeds the development of Web services.



Simultaneously, we are training your key users and administrators. So when our work is done, yours can go on.

IN THE END IT LOOKS LIKE THIS

Every solution will obviously be unique. But typically, you'll find a secure front-end employing the Sybase Enterprise Portal, with pre-built capabilities for list, filter and rules management, searches across applications and data stores, internal and external communications, management of the investigation process, maintenance of search and investigation histories and, of course, reporting and presentations.

Tying everything together is the Sybase Business Process Integrator (BPI) Suite

so you can quickly connect applications to other agencies or other financial institutions.

Get a complete solution that doesn't require you to start from scratch. We have the tools and skills to have you in compliance before October. And who could have an issue with that?

We can help you get started right away at www.sybase.com/integrationsolutions.



The Software Integration Company

We can help you integrate all the disparate data and business applications running in your enterprise and extend them to any location in the world: platforms, application servers, components, databases, applications, processes, integration brokers, even multi/virtualization solutions. By choosing Sybase, you can preserve and extend your existing infrastructure investments, avoid proprietary traps, and improve efficiency across the enterprise.

The USA PATRIOT Act contains strong measures to prevent, detect and prosecute terrorism and international money laundering, greatly expanding the breadth and depth of the law. Broadly stated, the act requires that financial institutions know their customers and, to the greatest extent possible, their customers' customers. Compliance for banks and securities dealers is required by October 2002. Non-compliance could involve costly civil and criminal penalties.

©2002 Sybase, Inc. All rights reserved. All trademarks are the property of their respective owners.

BETTER WHEN EVERYTHING WORKS TOGETHER.™

THE STRAIGHT GOODS ON SOFTWARE INTEGRATION.

The USA PATRIOT Act now presents everyone with an enormous information integration challenge. The experts agree that manual review processes for your customers and their financial transactions will no longer suffice. Non-compliance is not an option. The only question facing you is: who should you engage as your partner in implementing a solution?



THE SYBASE APPROACH

Our approach leverages the knowledge and capabilities we've developed over nearly 20 years of managing information, application and process integration.

The Sybase PATRIOTcompliance Solution helps you satisfy the integration requirements of the USA PATRIOT Act by implementing a totally automated process for filtering your customers, employees and suppliers against known suspects, and for continuously monitoring their activities. Our solution is operationally unobtrusive, secure and cost-effective.

THE FIRST STEP

Our first step is a Business Requirements Assessment that helps determine your organization's unique needs.

We work with you to understand your front and back office infrastructure. We embrace the technologies and product standardization of your environment. We extend the Anti-

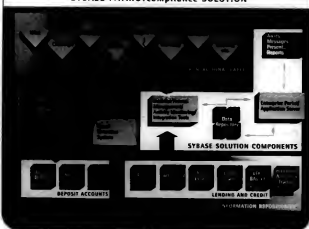
Money Laundering and Bank Secrecy Act investments you've already made. We make our solution work for your people.

Having tuned our PATRIOTcompliance Solution to your environment, we implement, rigorously test (to the very exacting standards we developed to earn ISO-9001/TickIT Certification) and deploy the solution

and an array of adapters (F.I.X., SWIFT, Flat Files, database, CICS, and others) for accessing and presenting demographic and transaction information from your core systems.

BPI Suite is a comprehensive set of tools to enable you to rapidly build, manage, monitor and improve complex business processes. It also speeds the development of Web services,

SYBASE PATRIOTcompliance SOLUTION



Simultaneously, we are training your key users and administrators. So when our work is done, yours can go on.

IN THE END IT LOOKS LIKE THIS

Every solution will obviously be unique. But typically, you'll find a secure front-end employing the Sybase Enterprise Portal, with pre-built capabilities for list, filter and rules management, searches across applications and data stores, internal and external communications, management of the investigation process, maintenance of search and investigation histories and, of course, reporting and presentations.

Tying everything together is the Sybase Business Process Integrator (BPI) Suite

so you can quickly connect applications to other agencies or other financial institutions.

Get a complete solution that doesn't require you to start from scratch. We have the tools and skills to have you in compliance before October. And who could have an issue with that?

We can help you get started right away at www.sybase.com/integrationsolutions.



The Software Integration Company

We can help you integrate all the disparate data and business applications running in your enterprise and extend them to any location in the world: platforms, application servers, components, databases, applications, processes, integration brokers, even mobile/wireless solutions. By choosing Sybase, you can preserve and extend your existing infrastructure investments, avoid proprietary traps, and improve efficiency across the enterprise.

The USA PATRIOT Act contains strong measures to prevent, detect and prosecute terrorism and international money laundering, greatly expanding the breadth and depth of the law. Broadly stated, the act requires that financial institutions know their customers and, to the greatest extent possible, their customers' customers. Compliance for bankers and securities dealers is required by October 2002. Non-compliance could involve costly civil and criminal penalties.

©2000 Sybase, Inc. All rights reserved. All trademarks are the property of their respective owners.

BETTER WHEN EVERYTHING WORKS TOGETHER.

A COMPUTER INCIDENT response team, or CIRT, is a lot like a firefighting crew — both are composed of individuals trained to respond quickly to specific incidents with the goal of limiting damage and reducing recovery time and costs.

"Like a fire department, you can use [CIRTs] for actual incident response and for cleanup, for education and for drills," says Richard Mogull, an analyst at GartnerG2 in Stamford, Conn.

With money and reputation on the line, a computer incident response team must be speedy and organized. By Jaikumar Vijayan



Build a Response Team

A CIRT may be activated by virus or hacker attacks, internal sabotage or even suspicious activity, such as successive attempts to gain access to a system or transactions that fall outside preset boundaries — such as a money transfer exceeding \$1 million.

Incident response at companies that don't have a CIRT tends to be reactive and ad hoc, says Steve Romig, manager of the network security group at Ohio State University in Columbus.

And there's more than money on the line. Companies that fail to react quickly

to security incidents stand to suffer damage to their reputations and lose customers.

A CIRT's key mission, therefore, is to orchestrate a speedy and organized company-wide response to computer threats. The following are some tips for building that capability:

KNOW YOUR CONSTITUENCY Decide which computers, address ranges and domains will be monitored for incidents, says Romig. Know what services the CIRT will provide and to whom. Develop policies for when to disclose security breaches and when to report an incident to law enforcement agencies, Romig says. And be sure to advertise contact information for the CIRT throughout the company, he adds.

ASSEMBLE THE TEAM Figure out which department the CIRT should be in and who should head it. Many companies put the team within the IT group, although others add the CIRT to the security or audit group, or make it a stand-alone function, says Georgia Kilcrease, a member of the CERT Coordination Center at Carnegie Mellon University in Pittsburgh.

"Wherever it sits, [a CIRT] will not succeed without management support," she says, because the team may require cooperation among multiple departments, such as legal and human resources.

The incident response team at the University of Wisconsin-Madison has a process for calling in its legal department and local law enforcement when incidents involve activities such as computer-related harassment, says Kim Milford, information security manager at the university.

Companies that can afford it sometimes maintain a formal team of specialists whose sole task is to respond to external and internal security breaches.

For example, one financial services firm has a core incident response team of 12 full-time specialists. Additional members are pulled in from the company's human resources and legal departments to assist this core team if necessary, says the company's IT director, who requested anonymity.

The University of Wisconsin-Madison has entrusted the task of coordinating incident response to one full-time worker. That person acts as a central point of contact for reporting and responding to incidents. Along with the university's IT security group, the employee is responsible for assessing the scope, priority and threat level of an incident, as well as for suggesting a response, Milford says.

CREATE A SWAT TEAM Maintaining a full-time incident response team can be expensive, so many companies choose to have an ad hoc incident response team that can come together quickly when needed, says Mogull.

Providence Health System creates SWAT teams to respond to specific incidents, such as virus infections, says David Rymal, director of technology at the Seattle-based health care provider.

"We use pager alerts and call an incident response meeting of the functional groups designated to respond to such incidents. At that meeting, we'll set a plan of action and a communication plan" for dealing with the threat, Rymal explains.

But, he adds, Providence Health System doesn't have formal methods of maintaining a CIRT beyond knowing the key players and who responds to which types of incidents.

GET ORGANIZED Have written policies and procedures and assign responsibilities upfront, says the financial services firm's IT director. "We maintain a formal list with names, cell phone numbers and beeper [numbers] of people who can be called in to assist the core team," he says.

Figure out what equipment you'll need, where you'll house it and how you'll protect the CIRT function. You don't want unauthorized people accessing information that a CIRT may uncover during a response, Kilcrease says.

None of this does any good if the plan merely sits on a shelf. Conduct frequent drills and mock exercises, especially for ad hoc teams, the financial services IT director says, adding, "Remember, it is a process that you have to do right but hope you never have to use." ▢

On Time. Up Time.
All the Time.

➡ www.nttverio.com/ad
Offering solutions with guaranteed results.

NTT/VERIO

NTT Communications Group Offices Japan • USA • Brazil • UK • France • Germany • Netherlands • Belgium • Switzerland
• Italy • Spain • Korea • China • Hong Kong • Taiwan • Vietnam • Thailand • Indonesia • Singapore • Malaysia • Philippines • Sri Lanka • Australia

*A full service offering may not be available in some areas.

NTT is a trademark of NIPPON TELEGRAPH AND TELEPHONE CORPORATION. Verio is a trademark of Verio Inc. America is a trademark of NTT Communications Corporation. All other referenced product names are trademarks of their respective owners. ©2002 NTT Communications Corporation

Forensics is neither pro-prosecution nor pro-defense; it's the pursuit of the truth.

MORRIS WINKLE, SENIOR INFORMATION SECURITY SPECIALIST AT UNISYS CORP. »



IT COULD BE A SERIES of erroneous corporate earnings statements or the unwitting loss of valuable trade secrets or customer data. It could be a string of sexual harassment allegations all pointing to one senior manager. Or it could be improper Internet usage that forces you to terminate an employee, who then sues for wrongful dismissal.

Whatever the cause, these potentially disastrous scenarios can be solved or proven only with the help of IT professionals with the right set of skills to investigate computer crimes.

Once thought of as the exclusive realm of violent-crime experts, forensics is fast becoming a mandatory skills set for companies that need to show that computer crimes don't go unsolved or unpunished. It's the painstaking and methodical sifting of data with one goal in mind: to gather evidence that will stand up in court. Here are some tips from the experts to make sure you win your case.

Lay the Legal Groundwork

Computer forensics is the identification, extraction, preservation and documentation of computer evidence that will stand up to legal challenges about its authenticity, accuracy and integrity. Think of it as an autopsy of a computer

Mistakes by a well-meaning IT staff could taint evidence and derail a court case. By Dan Verton

Let the Pros Investigate

Forensics for The Rest of Us

What managers should do first in a computer crime investigation

DO isolate the target system. Bring in legal support, and determine the scope of the investigation.

DON'T power on or boot up the system.

DO obtain copies of backup tapes from the local and regional IT departments within your company. Day, log and secure them.

DO preserve the data's evidentiary value by imaging and logging all hardware, storing it in a vault or secure area and keeping a log of access to evidence.

system with the goal of determining whether a crime has been committed and by whom and later proving it.

"Computer forensics is a process or methodology to discover or refute an area of inquiry," says Morgan Wright, a senior information security specialist at Unisys Corp. in Blue Bell, Pa., and a board member of the International Association of Computer Investigative Specialists in Donahue, Iowa.

Computer forensics is knowing, for example, that your company's trade secrets have been leaked to a rival and then proving or disproving that the employee you suspect of committing the breach is responsible. "Once you understand what the objective is, that's when you start your forensic investigation," says Wright. "Forensics is neither pro-prosecution nor pro-defense; it's the pursuit of the truth."

Hire Trained Investigators

Wright says the key difference between standard employee monitoring and a forensics investigation is the goal of preserving evidence that will stand up to legal challenges in court. He cites as an example the investigation of an acceptable-use violation, which might include looking into the user's history and proxy servers.

"On the other hand, let's say that same employee downloaded child pornography. Now, a system administrator who is not trained in forensics can accidentally trample over a lot of key evidence," says Wright.

The most common mistake that companies make when it comes to

computer forensics is thinking that their own systems administrators are capable of conducting a professional forensics investigation, says Thomas Aleman, national leader of analytic and forensic technology at Deloitte & Touche LLP's Computer Forensic and Investigative Services Group.

"The IT department is typically not trained and doesn't have the appropriate tools," says Aleman. "They turn on the machine under investigation, and as happens when machines are powered on, critical data starts changing."

In fact, Aleman recalls a case where the IT department at a large manufacturing firm was called in to recover data from the computer of a terminated employee who claimed to have been wrongfully dismissed. The administrators first turned on the suspect's computer. "The reality was that critical files had changed. And from a prosecution standpoint, the terminated employee was then in a position to argue that incriminating data was not in his system when he left," he says.

Aleman says other aspects of forensics investigations could trip up typical administrators. For example, local administrators at branch offices aren't always aware of the regional data backup schedules at larger companies, he says. That could pose a problem if defense lawyers question them about the version and timeliness of the data they're presenting in court.

Such oversights could seem minor to most IT managers, but they can mean the difference between a successful prosecution (or defense) in court and watching your case unravel, says Matt Yarborough, a former assistant U.S. attorney who spearheaded the formation of the North Texas Regional Computer Forensic Laboratory, the largest of its kind in the U.S. Of the 10 economic espionage cases brought to his office, only one made it to court, Yarborough says. The rest were undermined by tainted forensic evidence.

"As a prosecutor, there's nothing worse than a company that sponsors its own evidence in court," says Yarborough, who is now an attorney at Fish & Richardson PC in Dallas. "Being a super system administrator doesn't make you a forensics evidence expert capable of bringing evidence into the courtroom." ■

FORENSICS RESOURCES

Assisting in a forensics investigation can be a complicated business, but there are resources available to help.

📞 **Q&A: 30840**
www.computerworld.com

Forensics Tricks of the Trade

What the experts do first in a computer crime investigation:

1 SET UP LUNCHBOXES

According to Matt Yarborough, a former assistant U.S. attorney, forensics experts use "lunchboxes," or special computers plugged into the suspect's system that allow investigators to examine a machine without turning on its power and booting from the drive. A lunchbox creates a bit-by-bit, sector-by-sector mirror of the machine. It then produces reports that are generated by one of several software packages used by law enforcement agencies such as the FBI.

2 COPY SLACK SPACE

"Copying both active and unallocated space, called slack space, is also critical," says Kirsten Henneger, associate legal counsel and electronic discovery consultant at Eden Prairie, Minn.-based Ontrack Data International Inc. This is important because deleted files are never really deleted. They are merely stored in slack space.

3 RECORD THE CHAIN OF CUSTODY

Henneger also recommends creating an electronic log to record access to the original copy of the drive. This protects the chain of custody of the evidence. And before any analysis is conducted, she advises defining the scope of the investigation so as not to stumble into any privacy violations.

4 ISOLATE THE SUSPECT SYSTEM

Forensics investigations, especially ones that will produce admissible evidence, don't end after a copy of the suspect's hard drive is made. It's critical that the suspect system is locked down and isolated immediately, says Yarborough.

Once an image of the hard drive has been captured, the hard drive should be bagged and tagged, or placed in a container in a secure evidence vault with a seal that's properly labeled and dated to show that it hasn't been tampered with. All analyses should be conducted on the copies only.

At the end of the day, if it comes down to convincing a judge that the data you are presenting in court is in fact what you say it is, says Yarborough.

5 CREATE A TASK LIST

A thorough investigation can take anywhere from 20 to 30 hours, says Morgan Wright, a senior information security specialist at Unisys Corp. "Therefore, it's important to have a checklist and to conduct every step as if it's going to end up in court," he says.

6 USE AUTOMATION TOOLS ONLY TO SUPPLEMENT EXPERTISE

There are many automated tools to help with an investigation. They include Symantec Corp.'s Norton Data Edit, AccessData Corp.'s Forensic Tool Kit, Guidance Software Inc.'s Encase and Raytheon Co.'s Silent Runner. But, Wright warns, "you should not be using automation to [make up for] lack of experience."

— Dan Vortan

Watch Out For Wireless Rogues

Employees are bringing unsecured wireless LAN access points through the back door. Here's how to fight back. By Rob Brewin

TWENTY YEARS AGO employees starting stealing PCs into the office, under the radar of mainframe-oriented IT departments.

Now, tens of thousands of unauthorized wireless LAN hardware devices called access points (AP) have popped up in enterprise networks nationwide, according to analysts, vendors and users. The majority of these rogue APs are being brought in through the back door without the IT unit's knowledge. They're installed by employees who crave mobility and don't mind spending \$200 or less for a wireless AP.

It's "a classic example of technology bypassing corporate IT," says Brad Bray, director of network technology at ADC Telecommunications Inc. in Eden Prairie, Minn. But the proliferation of unauthorized APs is a far more serious threat than the stand-alone PCs that were brought in 20 years ago, he says.

These industry-standard 802.11b, or Wi-Fi, devices are plugged directly into an enterprise network, often behind a firewall. They transmit sensitive data that can be easily picked up by a

snoop using freeware hacking tools and a \$99 wireless LAN card while sitting in an office parking lot.

Sophisticated hackers don't even need to be near the premises to pick up a signal. Using long-range antennas — either commercial products or home-brew devices crafted from, say, Pringles potato-chip cans or coffee cans — they can pick up 802.11b signals from 1,000 to 2,000 feet away.

These serious hackers could be exploiting what analysts call "malicious" APs that are secretly installed in an Ethernet network by people who have easy access to property, such as maintenance personnel. Thor Sigvaldson, director of the advanced technology group at PwC Consulting in New York, says it's an easy form of industrial espionage. "You just stick one [wireless AP] into a network. It doesn't even need maintenance," he says.

Sigvaldson estimates that any U.S. enterprise, branch office, plant or store with more than 50 employees probably

has one or more rogue APs.

Bray says IT managers should adopt policies that welcome the wireless LAN technology but protect networks at the same time.

"We don't want to inhibit the technology, but we do want it installed in a secure fashion," he says. "We now have a policy against installing wireless LANs without corporate IT approval."

IT managers also have to engage in a time-consuming wireless AP "discovery process" to hunt down unauthorized installations, says Bray.

ADC initially sent staffers to walk around the company's 100-plus facilities worldwide with wireless LAN-equipped laptops and "sniffer" software to detect rogue APs. The staffers found an unspecified number of rogue APs in manufacturing facilities, but none in office operations, Bray says.

Vendors take various approaches to automating this process. AirDefense Inc. in Alpharetta, Ga., provides a suite of tools that make it easy to pinpoint the electronic signatures of the majority of wireless LAN APs and access cards on the market. The AirDefense tool set includes sniffers that can detect 802.11b transmissions, so that signatures of unknown APs can be compared to a database of authorized gear.

Finisar Corp. in Sunnyvale, Calif., recently introduced a wireless LAN spectrum analyzer that can help pinpoint unauthorized APs. IBM last month intro-

duced the Distributed Wireless Security Auditor, which uses authorized wireless clients as sensors to detect rogue APs (QuickLink 30667).

The Sniffer from Network Associates Inc. in Santa Clara, Calif., works from the wired side of the network, using tools such as Simple Network Management Protocol to determine the IP address of all wireless devices.

Securing wireless LANs against rogue APs and hackers can be costly.

How to Defend Against Rogue Access Points

POLICY

- Establish a no-exceptions policy against the use of wireless LANs without approval of the IT department.
- Set up an amnesty program that will allow employees to disclose their self-installed APs to the IT department within a one-month period.
- Encourage use of properly installed, configured and secured wireless LANs — if the business case justifies their use.

DISCOVERY

- Use sniffing tools to physically survey all facilities for wireless LAN signals, and then zero in on unauthorized devices.
- Don't ignore low-tech, small or obscure operations, such as truck terminals, loading docks, branch offices, factories and the maintenance department. It takes only one rogue AP to open up an enterprise network.

MAINTENANCE

- Continue to issue reminders of the no-exceptions policy.
- Swift premises periodically.
- Consider centrally managed systems for detecting rogue APs within large organizations.

says Chris Kozup, an analyst at Meta Group Inc. in Stamford, Conn.

"The cost of truly securing a wireless LAN will run anywhere from 10% to 100% of the hardware cost," Kozup says. "Once we walk customers through this, they sometimes decide wireless is too expensive." ■

WIRELESS LAN SECURITY

Learn about three products for detecting rogue wireless LAN APs.
 © QuickLink: 30856
www.computerworld.com

EXCLUSIVE COMPUTERWORLD SURVEY

Secrets in the Air

A survey of 159 IT professionals finds that almost half of them aren't confident that all of their wireless LAN access points are secured. And 30% have found rogue APs.

Are you confident that any and all wireless LAN APs in your organization have been identified and secured?



Do you have a written policy against employees installing their own wireless LAN networking gear (with-out IT department involvement)?



Have you identified any rogue wireless APs in your organization?



Do you "sniff" or monitor your corporate premises to determine the existence of rogue wireless APs?



Watch Out For Wireless Rogues

Employees are bringing unsecured wireless LAN access points through the back door. Here's how to fight back. By Bob Brewin

TWENTY YEARS AGO, employees starting sneaking PCs into the office, under the radar of mainframe-oriented IT departments.

Now, tens of thousands of unauthorized wireless LAN hardware devices called access points (APs) have popped up in enterprise networks nationwide, according to analysts, vendors and users. The majority of these rogue APs are being brought in through the back door without the IT unit's knowledge. They're installed by employees who crave mobility and don't mind spending \$200 or less for a wireless AP.

It's a classic example of technology bypassing corporate IT, says Dave Bray, director of network technology at ADC Telecommunications Inc. in Eden Prairie, Minn. But the proliferation of unauthorized APs is a far more serious threat than the stand-alone PCs that were brought in 20 years ago, he says.

These industry-standard 802.11b or Wi-Fi devices are plugged directly into an enterprise network, often behind a firewall. They transmit sensitive data that can be easily picked up by a

snooper using freeware hacking tools and a \$99 wireless LAN card while sitting in an office parking lot.

Sophisticated hackers don't even need to be near the premises to pick up a signal. Using long-range antennas — either commercial products or home-brew devices crafted from, say, Pringles potato-chip cans or coffee cans — they can pick up 802.11b signals from 1,000 to 2,000 feet away.

These serious hackers could be exploiting what analysts call "malicious" APs that are secretly installed in an Ethernet network by people who have easy access to property, such as maintenance personnel. Thor Sigvaldson, director of the advanced technology group at PwC Consulting in New York, says it's an easy form of industrial espionage. "You just stick one [wireless AP] into a network. It doesn't even need maintenance," he says.

Sigvaldson estimates that any U.S. enterprise, branch office, plant or store with more than 50 employees probably

has one or more rogue APs.

Bray says IT managers should adopt policies that welcome the wireless LAN technology but protect networks at the same time.

"We don't want to inhibit the technology, but we do want it installed in a secure fashion," he says. "We now have a policy against installing wireless LANs without corporate IT approval."

IT managers also have to engage in a time-consuming wireless AP "discovery process" to hunt down unauthorized installations, says Bray.

ADC initially sent staffers to walk around the company's 100-plus facilities worldwide with wireless LAN-equipped laptops and "sniffer" software to detect rogue APs. The staffers found an unspecified number of rogue APs in manufacturing facilities, but none in office operations, Bray says.

Vendors take various approaches to automating this process. AirDefense Inc. in Alpharetta, Ga. provides a suite of tools that make it easy to pinpoint the electronic signatures of the majority of wireless LAN APs and access cards on the market. The AirDefense tool set includes sniffers that can detect 802.11b transmissions, so that signatures of unknown APs can be compared to a database of authorized gear.

Finisar Corp. in Sunnyvale, Calif., recently introduced a wireless LAN spectrum analyzer that can help pinpoint unauthorized APs. IBM last month introduced the Distributed Wireless Security Auditor, which uses authorized wireless clients as sensors to detect rogue APs (QuickLink: 30667).

The Sniffer, from Network Associates Inc. in Santa Clara, Calif., works from the wired side of the network, using tools such as Simple Network Management Protocol to determine the IP address of all wireless devices. Securing wireless LANs against rogue APs and hackers can be costly,

How to Defend Against Rogue Access Points

POLICY

- Establish a no-exceptions policy against the use of wireless LANs without approval of the IT department.

- Set up an amnesty program that will allow employees to disclose their self-installed APs to the IT department within a one-month period.

- Encourage use of properly installed, configured and secured wireless LANs — if the business case justifies their use.

DISCOVERY

- Use sniffing tools to physically scan all facilities for wireless LAN signals, and then zero in on unauthorized devices.

- Don't ignore low-tech, small or obscure operations, such as truck terminals, loading docks, branch offices, factories and the maintenance department. It takes only one rogue AP to open up an enterprise network.

MAINTENANCE

- Continue to issue reminders of the no-exceptions policy.
- Sniff perimeter periodically.
- Consider centrally managed systems for detecting rogue APs within large organizations.

says Chris Kozup, an analyst at Meta Group Inc. in Stamford, Conn.

"The cost of truly securing a wireless LAN will run anywhere from 10% to 100% of the hardware cost," Kozup says. "Once we walk customers through this, they sometimes decide wireless is too expensive." ■

WIRELESS LAN SECURITY

Learn about free products for detecting rogue wireless LAN APs.
 Q: QuickLink: 30656
www.computerworld.com

Secrets in the Air

A survey of 198 IT professionals finds that almost half of them aren't confident that all of their wireless LAN access points are secured. And 30% have found rogue APs.

Are you confident that any and all wireless LAN APs in your organization have been identified and secured?



Don't know 19.2%

Do you have a written policy against employees installing their own wireless LAN networking gear (without IT department involvement)?



Don't know 10.7%

Have you identified any rogue wireless APs in your organization?

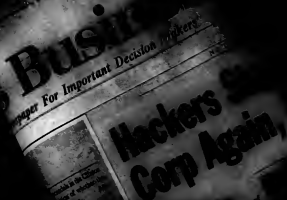


Don't know 12.6%

Do you "sniff" or monitor your corporate premises to determine the existence of rogue wireless APs?



Don't know 8.2%



When it comes to targeted hacker attacks, Trojan horses and spyware preying on your data, the last thing you want is to "read all about it." Hackers not only steal and destroy valuable information, they undermine your customer trust and brand equity—wounds that can leave you bleeding red ink.



Distributing IT resources across multiple locations could make it easier to recover from a disaster.

By James Cope

DISASTER PLANNING

THE TERRORIST ATTACKS on the U.S. last September fundamentally changed the way some IT managers think about disaster recovery.

"It's no longer a matter of planning what to do should fire or flooding prevent access to buildings," says Bob Fucito, vice president of crisis management and business continuity at investment banking firm BNP Paribas. Today, businesses have to prepare for the ultimate security risk: what to do when people and buildings are intentionally targeted and destroyed.

Fucito should know. His duties include managing disaster recovery for Paris-based BNP Paribas' North American operations. And he says he's thankful that his company's executives supported the creation of a disaster recovery plan that emphasizes distribution of IT resources — two years before the Sept. 11 attacks. The company had to evacuate its New York City building after the attacks, but Fucito says having two separate data centers and a contract with a hot-site recovery provider put BNP Paribas in a better position to continue doing business.

BNP Paribas isn't alone in thinking that having IT resources in one building or on a single network isn't a good idea. Other major organizations, such as The Boeing Co., United Air Lines Inc., the Chicago Board



of Trade and the U.S. Postal Service, try to mitigate the risk to IT resources by distributing data, applications and network infrastructure. They also have redundant communications links at the ready.

All of those organizations have the same goal: to quickly recover or even seamlessly continue doing business when disaster strikes. But they have different ways to accomplish it. Here are four approaches that major companies are using to stay prepared.

1 Redundancy and multiple routes: UAL Loyalty Services Inc. in Schaumburg, Ill., an online customer service unit of United Air Lines parent UAL Corp., is installing duplicate systems at two company-owned and -operated data centers. Both are in the Chicago area, says Igor Rafalovsky, director of networking and security, but the facilities are geographically separated. A metropolitan-area network capable of gigabit

Put Your IT In Different

speeds, known as a GigaMAN, connects the two centers, Rafalovsky says. Moreover, each data center is connected over T3 lines running to separate Private Network Access Points (P-NAPs), which are Internet backbone connection points owned and operated by Internap Network Services Corp. in Seattle.

And even at the P-NAPs, traffic going to and from the two UAL data centers runs across multiple Internet backbones from different providers, such as Sprint Corp., WorldCom Inc. and others. A P-NAP may have up to six or eight backbone providers online and available at any given time.

Both UAL data centers host Web servers, applications and databases. Disk storage is synchronized in real time over the GigaMAN, and both data centers are online all the time. "In the case of a catastrophic failure of one data center, the other one just picks up the traffic, in many cases without interruption... or manual intervention," Rafalovsky says.

2 Outsourced hot sites: When BNP Paribas IT employees evacuated their building in New York in response to the terrorist attacks, they moved to the company's other data center in New Jersey to continue operations. Even so, Fucito says his firm also has a contract with New York-based SchlumbergerSema to provide off-site hot sites.

Hot sites duplicate the mission-critical parts of a company's IT systems in secure buildings miles away from the primary sites. IT workers can go to hot sites to initiate recovery or simply resume work.

John Kersley, SchlumbergerSema's vice president of business recovery, describes how it works: A corporate customer configures its own data centers to automatically mirror data and applications to the appropriate hot-site recovery center (or centers). That company's IT employees are assigned physical positions (desks and workstations) at a specific center and instructed on how to get there if there's a crisis. When the company's workers are in place at the re-

Advanced Tips

■ **You can't predict disasters.** So be prepared for certain outcomes, such as being unable to enter the building.

■ **A disaster recovery plan should be simple, not a thick binder on a shelf.** It should fit on one sheet of paper or a single computer screen.

■ **The plan should say where employees should go, when to contact, which systems are likely to be affected and what to do about them.**

■ **Be realistic.** It may not be possible for a Fortune 1,000 company to recover from a major disaster in 24 hours.

SOURCES: ALAN PABLO, CAPCO; NEW YORK; CHARMAN WILCOX; SYRACUSE, N.Y.; LYLE, ILL.

covery center, it becomes a matter of patching the data through to the off-site desktops.

Hot sites are especially appealing to financial services organizations like BNP Paribas and the Board of Trade Clearing Corp., the clearinghouse for the Chicago Board of Trade, which has a hot-site contract with SunGuard Data Systems Inc. in Wayne, Pa.

The concept also has value for major retailers. For example, Leeds, England-based ASDA Group Ltd.—a Wal-Mart Stores Inc. in Bentonville, Ark.—has an agreement with SchlumbergerSema to send select members of its IT staff to a global business recovery center if a disaster closes ASDA's own IT facilities.

3 Blend of internal and external redundancy: SunGuard and SchlumbergerSema say the trend is toward using hot sites for disaster recovery. But Dominik Walch, vice president of consulting at T-Systems Inc. in Lisle, Ill., sees the trend heading in the opposite direction.

"Companies are looking at internalizing their disaster recovery systems and moving away from hot-site providers," Walch says. However, he acknowledges that the hot-site idea won't go away anytime soon and that disaster recovery strategies often involve a blend of approaches.

In fact, extremely large and diverse organizations, particularly those using mainframes in addition to PC servers, foster redundancy through a mix of multiple in-house data centers and mirrored hot sites.

Chicago-based Boeing, for example, has to consider the specific needs of business units and the communication challenges that come with having a multitude of far-flung locations.

"Distributed hot-site contracts tend to be more expensive with mainframe environments. We try to consolidate and centralize IT but also avoid the risk of too many megacenters... by having geographic separation [of IT facilities]," says Steve Gueck, Boeing's program manager for disaster recovery.

Gueck maintains that focusing on networks is the key to eliminating single points of failure.

4 Satellite backup: Bob Otto, vice president of IT at the U.S. Postal Service (USPS) in Washington, says he could see the smoke from his office after the aircraft struck the Pentagon on Sept. 11.

"We then evacuated our computer center of our Washington facility and set it up for remote management from our Raleigh [N.C.] disaster center and immediately instructed our data centers in California and Minnesota to begin backing up to Raleigh," Otto says.

Then Otto's group learned that the New York attacks had knocked out the frame-relay links connecting facilities in New York to the postal service's wide-area network. So the USPS pointed its VSAT satellite system toward New York, and the city's post offices were almost immediately back on the network.

It was all part of the plan, says Larry Willis, manager of distributed computing for the USPS. While frame-relay land lines are the primary network connection to thousands of post offices across the U.S., the USPS has 11,000 VSAT installations nationwide. Willis says. The VSAT services are provided by SpaceNet Inc. in McLean, Va.

Generally, the switch-over is automatic: When frame relay goes down, a satellite connection takes over. Willis says post offices generally don't even know when it has happened. ■

Cope is a Computerworld contributing writer. He can be reached at jc@jamescope.com.

PLAN AHEAD WITH THREE VIEWS OF DISASTER

Before a system goes down, determine how the loss of that system would affect people, technology and processes.

CircleLink 20093
www.computerworld.com

Eggs in Baskets

Denying Network Service

BY DEBORAH RADCLIFF

AT LEAST once each month, Terra Lycos SA's high-profile Internet media products, such as Lycos Mail, Tripod and Angelife, come under a denial-of-service (DOS) attack. As host to more than 300 distinct Web sites and 40.3 million users, the international hosting and Internet media company makes an obvious target, explains Tim Wright, chief technology officer and CIO at Terra Lycos' U.S. headquarters in Waltham, Mass.

The attacks aren't the traffic-clogging distributed denial-of-service (DDoS) attacks that used remote-controlled servers to flood Amazon, Yahoo, eBay and others with debilitating levels of traffic in early 2000.

Oldie but Baddie

The DOS attacks Wright sees are much older than that. They're called syn flood, a type of attack that has been around as long as TCP. Syn floods fake

the initial connection synchronization (syn) requests. The target responds with an acknowledgment (ack), for which it will receive no response. The target server holds the session open for a given length of time and then times out. A high-volume succession of these fake sessions prevents the machine from opening legitimate connections.

There's really no protection against syn floods, because they take advantage of the inherent purpose of routing protocols — to route TCP session connection requests. "The worst kind of attacks are where the protocol says it's normal," Wright explains.

Now, syn floods are getting a whole lot nastier. A new form of syn, called a distributed reflection denial-of-service (DRDOS) attack, knocked Laguna Hills, Calif.-based Gibson Research Corp. (GRC) off the Web for four hours in January.

A DRDOS attack is the inverse of a syn flood, says Steve Gibson, president of GRC. Gibson coined the term for the new attack method after his experience in January.

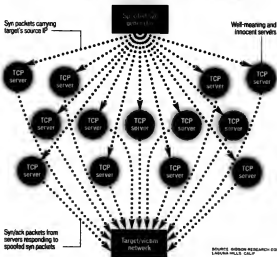
That's when attackers sprayed GRC.com's IP across core Internet routers and connected TCP devices, making them believe that GRC.com was trying to initiate a connection. Being the obedient devices that they are, they responded en masse to GRC.com with their ack replies. GRC.com's server, knowing that it didn't initiate the TCP session requests, simply dropped the acks. Thinking their ack requests were lost in cyberspace, the devices tried again — up to four times — magnifying the attack.

Gibson says he's aware of many companies that have come under such DRDOS attacks. "Web hosting sites and other major sites are the biggest targets," he says. "You up-

DEFINITION

Denial of service is a form of attack in which a network server is overloaded by thousands of false communications and/or requests for services originating from programs in one or more outside computers. Ultimately, the network receives so many queries that it can't keep up with them and is thus unavailable to answer or service legitimate requests.

The Distributed Reflection DOS Attack



SOURCE: BIRDSON RESEARCH CORP. LAGUNA HILLS, CALIF.

What Can You Do?

Syn flood remedies:

- Shorten how long a server will wait before timing out.
- Block traffic coming from the spoofed IP address.
- Use [iptables](http://www.gribble.org/iptables/iptables.html) (www.gribble.org/iptables/iptables.html) to prevent your network from being used as a spoofed IP address.

DRDOS remedies:

- At the time of the flood, ask your upstream service provider to "null route" packets coming at the IP. Unfortunately, this means dropping all packets coming into that IP address, which will result in a denial of service.
- Use traffic pattern analysis and network sniffers to help detect these attacks faster.

set some script kiddie — they especially don't like spammers — and they'll punish somebody."

Filtering doesn't help because it slows all traffic, say Wright and Gibson. In a DRDOS attack, the ack packets come from everywhere, so there's no way to filter.

The only way to deal with

such an attack is to take the target machine off the Web and wait it out, or ask your Internet service provider to "null route" (drop incoming syn or ack packets to the affected machine), Gibson explains. That way, the attackers can't block traffic to other machines on that network segment. But then, he adds, "the

attacker's still won. They've shut your site down."

MORE JARON ONLINE

For a glossary of related terms, visit [Computerworld.com](http://www.computerworld.com).

QuickStart Link: SYNIDS
www.computerworld.com

Are there technologies or issues you'd like to learn about in QuickStudy? Send your ideas to quickstudy@computerworld.com

PRODUCED BY
COMPUTER WORLD

STORAGE
NETWORKING
WORLD
ONLINE

ENDORSED BY
SNIA

www.snwonline.com/300



WITHOUT BORDERS

NICHOLAS PETRELEY

Think Like a Terrorist

I WAS WORKING from my home office a few years ago when my access to a Web site called NC World was suddenly cut off. My service provider told me that a router in Southern California had gone down. This struck me as odd for two reasons. First, I live in Northern California, about a half-hour from San Francisco, where NC World was hosted at the time. Second, I was under the impression that one of the primary design goals for the Internet was to make sure that communications would proceed uninterrupted even if some of the primary hubs are taken out by a nuclear blast.

I have no idea what really caused this temporary outage, but I assume it occurred because of a minor hardware failure or administrator error. But if Internet communications are this easily interrupted by accident, I can't help but conclude that we are totally unprepared for the consequences of an intelligent, direct attack by cyberterrorists.

Here's how you can prevent such an attack: Think like a terrorist. Look at trends, and explore every possible opportunity and method possible to launch an attack on the U.S. infrastructure and economy. Then put your IT hat back on and plan ahead to prevent these methods from working.

Here's an example. One inevitable trend is the increase in business-to-business transactions over the Internet, a trend that will only be fortified by the advancement of Web services. Let's assume, for the sake of argument, that within two to 10 years, most business-to-business transactions will take place over the Internet. If I were a cyberterrorist, I would plan now for the day when I could disrupt as many of these business-to-business transactions as possible. Depending on how many servers I could bring down and

for how long, I could create big headlines, delay or halt shipments, or perhaps even do lasting damage to the economy.

The obvious method is to launch a distributed denial-of-service attack. That would get me the most bang for the buck. I don't have to defeat firewalls, gain administrator access to business computers or crack any Web services to launch this kind of attack. All I have to do is overwhelm carefully selected servers or just as many servers as possible.

So, how do I distribute the attack software? Microsoft's business model is the most promising. Microsoft makes its money by putting its products in the hands of as many people as possible, after which it charges everyone in the service chain a nickel. Its latest plan revolves around turning the Xbox game console into a home entertainment center, after which it can charge co-tenant providers for the digital rights management

they so desperately need in order to protect their revenue streams.

Microsoft needs only two things to happen to make this work: It must get the Xbox into 100 million homes or more, and the cost of broadband access to the Internet has to drop to within reach of the average household.

You should be able to see where I'm going with this by now. If you wanted to launch the ultimate denial-of-service attack, what more could you ask for than 100 million Xbox units with broadband access to the Internet, all running software developed by the "crack me" specialists of the world? Now, what's the cure?

I'm afraid to disappoint those of you who are expecting a knee-jerk anti-Microsoft response, but making the Xbox wouldn't solve anything. Microsoft is depending on getting its software into every home one way or another, so the best answer is to prepare for that day.

For one thing, I would pressure everyone necessary to standardize and implement quality-of-service (QoS) protocols. Demand that your ISP support QoS. Implement QoS as part of your plans for Web services. Most important, pressure vendors to implement QoS in hardware whenever possible, especially for high-volume consumer devices like game machines, cell phones or anything else that can connect to the Internet. If the hardware wraps every packet in a low-priority envelope, nobody can trick an Xbox or any other consumer device into generating data that takes precedence over the information that runs our country.

This is only one example and one possible solution. How many can you think of?



Learn how a network assessment can help you discover how close you are to IP Telephony. Visit avaya.com/yus

AVAYA

COMMUNICATION WITHOUT BOUNDARIES

Out From the Shadows

What's a VPN?

QUICK STUDY

A virtual private network (VPN) is a network connection that has the appearance and many of the advantages of a dedicated link but is in fact implemented over a shared network. Using a technique called tunneling, data packets are transmitted across a public routed network such as the Internet. Generally, the private network data and protocol information are carried inside a wrapper so that along the way, they look like data to the routers, which remain un-

aware that the transmission is part of a private network. Only when the transmission reaches its destination is it unwrapped and sent to its intended recipient. This private "tunnel" simulates a point-to-point connection, and it allows network traffic from many sources to travel via separate tunnels across the same infrastructure.

Tunneling allows network protocols to traverse incompatible infrastructures. It also enables traffic from many sources to be differentiated so that it can be directed to specific destinations

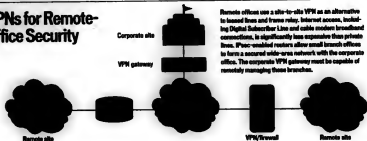
and receive specific levels of service.

Tunneling can be initiated by a variety of network devices and software, such as an end user's laptop equipped with an analog PC modem card and VPN-enabled dial-up software. (Basic tunneling and security capabilities have been bundled into Windows since the release of Windows 95.)

Tunnels can also be started by a VPN-enabled extranet router on an enterprise branch or home office LAN, or by a VPN-enabled access concentrator at a network service provider's point of presence. A tunnel is ended by a tunnel terminator or switch on an enterprise network, or by a VPN gateway on a network service provider's network extranet router.

In addition, there are usually one or more security servers. Along with their conventional functions as firewalls and address translators, VPNs can provide for data encryption, authentication and authorization. Tunneling devices perform these functions by communicating with security servers. Such servers also usually provide information on bandwidth, tunnel end points and, in some cases, network policy information and service levels. ■

VPNs for Remote-Office Security



Remote offices use a site-to-site VPN as an alternative to leased lines and frame relay. Internet access, including Digital Subscriber Lines and cable modem broadband services, is significantly less expensive than private lines. IPsec-enabled routers allow small branch offices to form a secured wide-area network with the corporate office. The corporate VPN gateway must be capable of remotely managing these branches.

The Battle for Mainstream Acceptance

TECH CHECK

Providing secure remote access and telecommunications over the Internet to remote workers is a fact of life in modern business, and virtual private networking is the primary technology making that possible. IT managers have had trouble adopting VPNs because of deployment issues, compatibility and interoperability problems and the expense of these systems.

That has changed. VPNs are entering the mainstream, and many companies view them as a telecommunications necessity from both security and cost perspectives. In fact, Framingham, Mass.-based IDC's "2001 WAN Manager Survey," published in December, concluded that IP VPNs are now a mainstream wide-area network option for most businesses. And browser-based Secure Sockets Layer VPNs are

growing in popularity because they require little or no additional software or firewall reconfiguration.

"The trend has been to create VPNs for remote access, since they offer considerable cost reductions over toll-free numbers and in-house [remote access servers]," says Dave Kostur, a senior analyst at Burton Group in Midvale, Utah.

But that's not to say that enterprise VPNs have no rough edges. Depending on the type of technology and products selected, VPNs can still cause headaches and force companies to outsource deployment and management to service providers.

Increasingly, the VPN and firewall markets have been merging, as hardware-based implementations have continued to dominate. But interoperability between products from different vendors remains one of the VPN market's biggest challenges. It's also

a challenge for large enterprises that may want or need to use different hardware and operating systems in different locations.

"The outlook for interoperable devices and software is improving, although it's only natural for vendors to try and lock customers into only their product line," says Kostur. "There will always be value-added features in different vendors' products that will inhibit 100% interoperability."

Interoperability problems are "preventing the VPN market from meeting its potential," says Leo Phawick, technology program manager

at ICSS Labs, a testing clearinghouse for VPN and firewall technologies in Mechanicsburg, Pa. "Each vendor develops to target a particular business problem. Large-scale, interoperable deployments are a goal, not a reality yet." ■

ANSWERS ONLINE

Links to VPN resources:
QuickLink: 31040

A list of VPN vendors:
QuickLink: 31040

Q&A with analyst Dave Kostur:
QuickLink: 31040
computerworld.com

Shadows

A Crowded, Confused Market

Dedicated VPN hardware revenues totaled \$1.3 billion in 2001 and are forecast to reach \$2.9 billion in 2005, according to a study published in February by Infonetics Research in San Jose.

End users of all types and sizes are also buying managed VPN and security services, representing a lucrative opportunity for all types of service providers, according to Infonetics.

But the market is crowded, and it can be confusing. Some service providers offer only security, some offer only VPNs, and some offer both. Some vendors simply deploy and manage security and VPN devices; others actively monitor the network and provide the customer with an analysis of potential

security gaps. There are also providers that offer services based on the equipment customers have in-house, vs. those that have network-based services or a blend of services on customer equipment and network-based services.

There are other barriers that the market must overcome. Many buyers are overwhelmed by the multitude of products available and the overcrowded service provider space.

"The market is real, but the market leaders for products and services have yet to truly emerge, and 2002 will be a critical year for product manufacturers and service providers to prove they can satisfy customer requirements," the Infonetics study concluded. ■

COMPETITION

Outsourcing Can Help

FIELD NOTES

The growth of e-business and the ever-increasing integration between corporations and their suppliers and trading partners has put a premium on security, user authentication and data integrity. In addition, recent economic pressures have forced many companies to reassess their telecommunications strategies with an eye not just toward security, but toward cost and performance as well.

Users are turning to VPNs as an answer to all of these challenges. In addition to providing increased security, in some cases VPNs have reduced telecommunications management costs and improved performance. However, deploying a VPN isn't like deploying a few new desktop PCs. There are still many technical challenges to work out and much research to do before you choose any one VPN product or architecture, says users.

"We were worried about the technological risk associated with the changing technology," says Ed Flynn, CIO at FMC Corp., a Philadelphia-based manufacturing company with 90 locations worldwide. FMC started the move toward a VPN in early 2000 as a means to provide what Flynn calls "secure anywhere, anywhere access" for more than 1,000 employees. However, the growth of business-to-business trading also increased concerns about having to

touch customer systems, says Flynn, "and we didn't want to do that at all."

After researching its options, FMC chose Seattle-based Avenet Corp. for its VPN and remote access requirements. It came down to the technology choice. Flynn says. The Avenet service allows FMC to control employee access rights and also uses a nonlawyer agent that leaves the client IP stack alone, thereby meeting FMC's requirement to not touch customer systems.

"We vetted who we went with very well," says Flynn, "so we're not limited by the technology choice." And since FMC "had no idea how to deploy what they needed on their own," handing over these complex technologies to a company with the know-how minimized the risk, he explains.

Kelly Henderson, chief operating officer at AutoWeb Communications Inc. in Oak Park, Mich., agrees with the idea of having someone else do the VPN work. AutoWeb, which does business through a VPN managed by Southfield, Mich.-based ANKLab Inc., was faced with figuring out a tunnel management process for each of its 600 trading partners, including nine of the world's largest automotive manufacturers.

"Most companies aren't in the business of managing telecommunications," says Henderson. "It's not their

Healthy Connections

Spectrum Health
Grand Rapids, Mich.

WHO THEY ARE: A large, regional integral of health care system serving 13 western Michigan counties and 1.36 million people.

GOAL: To meet the new security requirements called for by the Health Insurance Portability and Accountability Act and to manage 5,000 independent (nonemployee) users.

CHALLENGES: Spectrum has more than 60 locations in 13 counties, including seven hospitals. The network has to serve 12,000 employees and more than 1,000 independent physician's offices. Thus, minimizing risk was one of the primary concerns, says Jim Toth, director of technology services.

"While we could cobble together some [homegrown] solutions, we were constantly running into challenges in encryption, tunneling and protection of our protected network zone," says Toth. Without a VPN, Toth would have had to open up 50 ports into

his network's protected zone, which would have been a very insecure approach.

STRATEGY: Toth chose technology from AppGate Inc. in Durham, N.C., that established a link between terminal emulation software and the client PCs. The AppGate product, based on the Secure Shell protocol, based on either IPsec or Secure Socket

CASE STUDY

Layer, provides a tunnel at the application layer, not just the network layer, and includes 128-bit encryption.

"Automatically, we have a secure tunnel at the application layer where I wanted to have it," says Toth. "We really limit our points of access."

ISSUES: Even with assistance from vendors and service providers, Toth acknowledges that VPNs can be "fairly complex" systems to set up.

PROOF: "This was really a functional issue," says Toth. "It's not so much about saving money. I don't think I could have offered a solution without a VPN."

core business." And VPN tunnel management on AutoWeb's scale "can get involved" and "can be a significant investment for companies," she says.

"There's expertise that we didn't have but that we needed to have to handle that type of process," says Henderson. "The cost is well worth it to us because of the type of business we're in. But you need to identify where the real pain points are and whether a VPN is going to address those pain points."

Joe Klein, director of telecommunications at Illinois Tool Works Inc. (ITW) in Glenview, Ill., says deploying a VPN hasn't been painful; in fact, he says it's been a pleasant, cost-effective change from traditional telecommunications methods.

ITW deployed a VPN from OpenReach Inc. in Woburn, Mass., to replace frame-relay networks connecting up to 70 business units. VPN tunnels are supporting human resources, financial and e-mail

applications between remote sites and ITW's headquarters, as well as 100 remote dial-in users.

"Users have to realize that with all good things, it takes some time to accommodate change and get used to the product," says Klein, noting that he made use of the OpenReach installation team to get the VPN up and running. However, so far the VPN has helped Klein cut costs by 30% to 50%, he says. ■

You need to identify where the real pain points are and whether a VPN is going to address [them]

Out From the Shadows

What's a VPN?

A few short years ago, the mention of virtual private networks would send network and security administrators running for cover. VPNs were too difficult to deploy correctly, the technology wasn't mature, and the return on investment was negligible. Now, what a difference. Today, VPNs are well accepted, and indeed, many companies view them as a necessity for both security and cost reasons.

QUICK STUDY

A virtual private network (VPN) is a network connection that has the appearance and many of the advantages of a dedicated link but is in fact implemented over a shared network. Using a technique called tunneling, data packets are transmitted across a public routed network such as the Internet. Generally, the private network data and protocol information are carried inside a wrapper so that along the way, they look like data to the routers, which remain un-

aware that the transmission is part of a private network. Only when the transmission reaches its destination is it unwrapped and sent to its intended recipient. This private "tunnel" simulates a point-to-point connection, and it allows network traffic from many sources to travel via separate tunnels across the same infrastructure. Tunneling allows network protocols to traverse incompatible infrastructures. It also enables traffic from many sources to be differentiated so that it can be directed to specific destinations

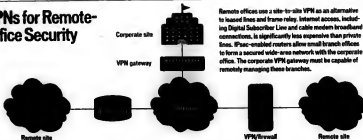
and receive specific levels of service.

Tunneling can be initiated by a variety of network devices and software, such as an end user's laptop equipped with an analog PC modem card and VPN-enabled dial-up software. (Basic tunneling and security capabilities have been bundled into Windows since the release of Windows 95.)

Tunnels can also be started by a VPN-enabled extranet router on an enterprise branch or home office LAN, or by a VPN-enabled access concentrator at a network service provider's point of presence. A tunnel is ended by a tunnel terminator or switch on an enterprise network, or by a VPN gateway on a network service provider's network extranet router.

In addition, there are usually one or more security servers. Along with their conventional functions as firewalls and address translators, VPNs can provide for data encryption, authentication and authorization. Tunneling devices perform these functions by communicating with security servers. Such servers also usually provide information on bandwidth, tunnel end points and, in some cases, network policy information and service levels. ■

VPNs for Remote-Office Security



The Battle for Mainstream Acceptance

TECH CHECK

Providing secure remote access and telecommunications over the Internet to remote workers is a fact of life in modern business, and virtual private networking is the primary technology making that possible. IT managers have had trouble adopting VPNs because of deployment issues, compatibility and interoperability problems and the expense of these systems.

That has changed. VPNs are entering the mainstream, and many companies view them as a telecommunications necessity from both security and cost perspectives. In fact, Framingham, Mass.-based IDC's "2001 WAN Manager Survey," published in December, concluded that IP VPNs are now a mainstream wide-area network option for most businesses. And browser-based Secure Sockets Layer VPNs are

growing in popularity because they require little or no additional software or firewall reconfiguration.

"The trend has been to create VPNs for remote access, since they offer considerable cost reductions over toll-free numbers and in-house (remote access servers)," says Dave Kosiarz, a senior analyst at Burton Group in Midvale, Utah.

But that's not to say that enterprise VPNs have no rough edges. Depending on the type of technology and products selected, VPNs can still cause headaches and force companies to outsource deployment and management to service providers.

Increasingly, the VPN and firewall markets have been merging, as hardware-based implementations have continued to dominate. But interoperability between products from different vendors remains one of the VPN market's biggest challenges. It's also

a challenge for large enterprises that may want or need to use different hardware and operating systems in different locations.

"The outlook for interoperable devices and software is improving, although it's only natural for vendors to try and lock customers into only their product line," says Kosiarz. "There will always be value-added features in different vendors' products that will inhibit 100% interoperability."

Interoperability problems are "preventing the VPN market from meeting its potential," says Leo Plushwick, technology program manager

at ICSA Labs, a testing clearinghouse for VPN and firewall technologies in Mechanicsburg, Pa. "Each vendor develops to target a particular business problem. Large-scale, interoperable deployments are a goal, not a reality yet." ■

ANSWERS ONLINE

Links to VPN resources
QuickLink: 31048

A list of VPN vendors
QuickLink: 31048

Q&A with Crystal Baller Kosiarz
QuickLink: 31048

computerworld.com

shadows

A Crowded, Confused Market

Dedicated VPN hardware revenues totaled \$1.3 billion in 2001 and are forecast to reach \$2.9 billion in 2005, according to a study published in February by Infonomics Research in San Jose.

End users of all types and sizes are also buying managed VPN and security services, representing a lucrative opportunity for all types of service providers, according to Infonomics. But the market is crowded, and it can be confusing. Some service providers offer only security, some offer only VPNs, and some offer both. Some vendors simply deploy and manage security and VPN devices; others actively monitor the network and provide the customer with an analysis of potential

security gaps. There are also providers that offer services based on the equipment customers have in-house, vs. those that have network-based services or a blend of services on customer equipment and network-based services.

There are other barriers that the market must overcome. Many buyers are overwhelmed by the multitude of products available and the overcrowded service provider space.

"The market is real, but the market leaders for products and services have yet to truly emerge, and 2002 will be a critical year for product manufacturers and service providers to prove they can satisfy customer requirements," the Infonomics study concluded. ▀

COMPETITION

Outsourcing Can Help

FIELD NOTES

The growth of e-business and the ever-increasing integration between corporations and their suppliers and trading partners has put a premium on security, user authentication and data integrity. In addition, recent economic pressures have forced many companies to reassess their telecommunications strategies with an eye not just toward security, but toward cost and performance as well.

Users are turning to VPNs as an answer to all of these challenges. In addition to providing increased security, in some cases VPNs have reduced telecommunications management costs and improved performance. However, deploying a VPN isn't like deploying a new desktop PCs. There are still many technical challenges to work out and much research to do before you choose any one VPN product or architecture, say users.

"We were worried about the technological risk associated with the changing technology," says Ed Flynn, CIO at FMC Corp., a Philadelphia-based manufacturing company with 90 locations worldwide. FMC started the move toward a VPN in early 2000 as a means to provide what Flynn calls "secure anywhere, anywhere access" for more than 1,000 employees. However, the growth of business-to-business trading also increased concerns about having to

touch customer systems, says Flynn, "and we didn't want to do that at all."

After researching its options, FMC chose Seattle-based Aventail Corp. for its VPN and remote access requirements. It came down to the technology and flexibility, says Flynn. The Aventail service allows FMC to control employees, access rights and also uses a noninteractive agent that leaves the client IP stack alone, thereby meeting FMC's requirement to not touch customer systems.

"We vetted who we went with very well," says Flynn. "So we're not limited by the technology choice." And since FMC "had no idea how to deploy what they needed on their own," handing over these complex technologies to a company with the know-how minimized the risk, he explains.

Kelly Henderson, chief operating officer at AutoWeb Communications Inc. in Oak Park, Mich., agrees with the idea of having someone else do the VPN work. AutoWeb, which does business through a VPN managed by Southfield, Mich.-based ANXebusiness Corp., was faced with figuring out a tunnel management process for each of its 600 trading partners, including nine of the world's largest automotive manufacturers.

"Most companies aren't in the business of managing telecommunications," says Henderson. "It's not their

Healthy Connections

Spectrum Health
Grand Rapids, Mich.

WHO THEY ARE: A large regional integrated health care system serving 13 western Michigan counties and 1.38 million people

GOAL: Meet the new security requirements called for by the Health Insurance Portability and Accountability Act and to manage 5,000 independent (nonemployee) users

CHALLENGES: Spectrum has more than 60 locations in 13 counties, including seven hospitals. The network has to serve 12,000 employees and more than 1,000 independent physician's offices. Thus, minimizing risk was one of the primary concerns, says Josh, director of technology services.

"While we could cobble together some [homegrown] solutions, we were constantly running into challenges in encryption, tunneling and protection of our protected network zone," says Josh. Without a VPN, Josh would have had to open up 50 ports into

the network's protected zone, which would have been a very insecure approach.

STRATEGY: Toth chose technology from AppGate Inc. in Durham, N.C., that established a link between terminal emulation software and the client PCs. The AppGate product, based on the Secure Shell protocol rather than Psec or Secure Sockets Layer, provides a tunnel at the application layer, not just the network layer, and includes 128 bit encryption.

CASE STUDY "Automatically, we have a secure tunnel at the application layer where I wanted to have it," says Josh. "We really limit our points of access."

ISSUES: Even with assistance from vendors and service providers, Josh acknowledges that VPNs can be "fairly complex" systems to set up.

PIVOT: "This was really a functional issue," says Josh. "It's not so much about saving money. I don't think I could have offered a solution without a VPN."

core business." And VPN tunnel management on AutoWeb's scale "can get involved" and "can be a significant investment for companies," she says.

"There's experience that we didn't have but that we needed to have to handle the type of process," says Henderson. "The cost is well worth it to us because of the type of business we're in. But you need to identify where the real pain points are and whether a VPN is going to address those pain points."

Joe Klein, director of telecommunications at Illinois Tool Works Inc. (ITW) in Glenview, Ill., says deploying a VPN hasn't been painful; in fact, he says it's been a pleasant, cost-effective change from traditional telecommunications methods.

ITW deployed a VPN from OpenTeach Inc. in Webport, Mass., to replace frame-relay networks connecting up to 70 business units. VPN tunnels are supporting human resources, financial and e-mail applications between remote sites and ITW's headquarters, as well as 100 remote dial-in users.

"Users have to realize that with all good things, it takes some time to accommodate change and get used to the product," says Klein, noting that he made use of the OpenTeach installation team to get the VPN up and running. However, so far the VPN has helped Klein cut costs by 30% to 50%, he says. ▀

You need to identify where the real pain points are and whether a VPN is going to address [them].

BY KATHLEEN A. GALLAGHER
CONTRIBUTOR

Guardians of The Gate

What you need to know to land a job and keep your skills fresh in the IT security field. By Amy Helen Johnson

Employee Spotlight

Name: JONATHAN TAYLOR

Title: Enterprise security engineer

Company: Sutter Health, Sacramento, Calif., a nonprofit services organization for 25 affiliate hospitals in Northern California

300-second résumé: Taylor has worked in IT since 1994. After graduating from Brigham Young University in Provo, Utah, he joined a value-added reseller. While moonlighting as a Windows NT Server instructor at MTI College of Business and Technology in Sacramento, a fellow teacher told him about an opening at Sutter Health. He joined the company in 1997, first working on a project to roll out a Windows NT platform throughout the company's health care affiliates. Taylor switched to IT security in early 2000.

Skills bonus: On-the-job training is the best way to learn, says Taylor. "There's very little training for information security," he says. "And even if there was, it's such a vast field that it would be difficult to get what you need for your particular industry or job."

ON-THE-JOB training is best, says Jonathan Taylor of Sutter Health.

CAREERS

Still, Taylor has found some courses that help him keep current. His most recent training came from Foundation Inc., a security services firm in Mission Viejo, Calif. At its Web hacking course, he learned about common Web site vulnerabilities that hackers exploit - vulnerabilities that existed within Sutter Health's public site. "It was a great big eye-opener,"

he says.

Other resources that Taylor uses to learn about potential security risks are newsgroups and Web sites devoted to IT security. He says there's a helpful bug list on the Web site of San Mateo, Calif.-based SecurityFocus.

Taylor says the mechanics of his job haven't changed since the events of Sept. 11, what's different is the interest that company executives now have in security. "When we would see patterns of risk before 9/11, people were apt to dismiss it," says Taylor. "Now when we say we have a concern, people's eyes go wide open."

-Johnson is a contributing writer in Seattle.



Best Place

■ A financial services company focused on business and private banking and investment services.

■ Ranked No. 9 on Computerworld's 2002 Best Places to Work in IT list.

■ 2001 revenue: \$4.2 billion

■ Number of IT workers: 800; 19 in IT security

MANAGER'S VIEW: Comerica doubled the size of its IT security team during the past 18 months, says Ken Schaeffler, first vice president. The bank switched from an IT infrastructure that supported only employees to one that provided online services to its customers.

Security concerns changed from an emphasis on access - IDs and passwords - to identifying the vulnerabilities associated with Internet-based applications, he says. Specialty departments for security administration, security architecture, risk management, regulations monitoring, and policies and procedures handle the bank's increased security needs.

The bank encourages IT security employees to get CISSP certification and will pay for the coursework and testing. More than 60% of the security staff is certified, says Schaeffler.

Training opportunities are well funded and popular with employees and are considered a key retention tool, he adds.

STOP HACK ATTACKS

One security engineer offers his tips for staying a step ahead of the hacker community.

QuickLink: 30029
www.computerworld.com



The Next Chapter

Pundits predict the rise of 'security malpractice' lawsuits but foresee sluggish growth for smart cards.

■ UNCLE SAM WILL AUDIT YOU

The U.S. government will create a cyber equivalent of the Transportation Security Administration (TSA). Just as the TSA is charged with elevating the current level of transportation security nationwide in all modes — air, land, water and rail — so, too, will the Digital Security Administration be charged with elevating the current level of digital security being practiced by commercial enterprises in the U.S.

The Digital Security Administration will conduct information security audits on the code of the top 20 enterprise software vendors. Code not found to be up to specifications will be labeled unsafe. Vendors with unsafe code will have six months to bring the code up to security standards.

The Digital Security Administration will also conduct information security audits at all companies in the critical infrastructure:

- Financial and currency markets.
 - Domestic and global lines of communication.
 - Mass points of e-sale and retail.
 - Utilities.
 - Health care facilities.
- Failure to bring code, data and network management practices up to specification will result in jail sentences for board members and senior executives.

— Thornton A. May, Toffler Associates Inc., Manchester, Mass.

■ NATIONAL IT SECURITY COUNCIL?

By 2010, IT security will become the

primary focus of U.S. national security policy.

— Atul Dholake, senior futurist, Institute for Alternative Futures, Alexandria, Va.

■ 90% OF THE PROBLEM

Through 2005, 90% of cyberattacks will exploit known security flaws for which a patch is available or a solution known.

And through 2005, 20% of enterprises will experience a serious Internet security incident (beyond a virus). Of those that do, the cleanup costs of the incidents will exceed the prevention costs by 50%.

— Richard Mogull, analyst, Gartner G2, Stamford, Conn.

■ ON THE CEO AGENDA

IT security will become a boardroom issue in the next two years. CEOs will have to manage the risks, just as they manage other sorts of risks. They'll depend on chief security officers to provide the metrics on a portfolio of assets and the risks that have a bottom-line impact — just like a chief financial officer does, except that IT risks are constantly changing.

— Mark Milatovich, director of security, Corio Inc., San Carlos, Calif.

■ NOT AN IN-HOUSE JOB

Security will be outsourced, as more and more companies realize it's too expensive to do in-house. Just as companies outsourced their software 20 years ago or their modem banks five years ago, they will outsource their network infrastructures tomorrow.

row. In the real world, every bank hires another company to drive its money around town, and every building manager hires another firm to post guards in its lobby. Outsourced network security will become as commonplace as outsourced phone services are today.

— Bruce Schneier, founder and chief technology officer, Counterpane Internet Security Inc., Cupertino, Calif.

■ THE BIOMETRIC NICHE

Stronger authentication will supplement simple password approaches in the next few years, but infrastructure limitations will impede smart card adoption until 2003, and biometrics will remain niche through 2005.

— Earl Perkins, analyst, Meta Group Inc., Stamford, Conn.

■ SMART CARDS: SLOW GROWTH

Significant smart card growth still faces several hurdles. Issuers are hesitant to commit to smart cards until the cost of the chip card comes down. Merchants won't spend the money to upgrade equipment to accept cards because they don't see consumer demand. And consumers don't yet see why they need a chip card — no one has come up with the right combination of chip-based applications to integrate them enough to switch.

— Catherine Gruber, analyst, Forrester Research Inc., Cambridge, Mass.

■ MALPRACTICE LITIGATION

What do you tell the CEO when a forensic audit of your public relations disaster says it could have been prevented by a vendor fix that had been available for eight months but was never applied?

Food for Thought

A technology timeline from British futurists forecasts a world of cyberwarfare.

2005: Crime and terrorism are mainly computer-based.

2005: Use of quantum cryptography is in effect.

2006: Public-key cryptography is cracked within a few seconds.

2007: First Internet war between cybercommunities begins.

2008: Robotic security and fire guards are implemented.

2010: Most weapons attack systems rather than human people.

2010: First Internet war between cybercommunities begins.

Ineffective application of hardware and software security fixes is career-threatening. Chief security officers who fail to get their arms around configuration and change management will exceed the CIO turnover rate of 38% by 2003.

This is what breeds those "left to seek other opportunities" memos and will produce a lot of security malpractice litigation in the next two to five years.

— Phil Rouse, analyst, Giga Information Group Inc., Cambridge, Mass.

Touchy Subject

A biometric gadget the size of a car alarm remote control could not only unlock cars and homes but also validate credit card transactions on the fly, according to Cross Match Technologies Inc. in Palm Beach Gardens, Fla.

A working model of the *Authorizer*, as it's called, is still two and a half years away. The company hopes to lower the price to \$50 apiece. The device will read the user's fingerprint and send it wirelessly to a third-party for authentication. The *Authorizer* will have another layer of security as well: It will be able to sense the blood flow in a finger.

That's important, because it means the finger must be attached to a living person (not a cast). And if the blood is flowing faster than normal — for example, if the user is being held at gunpoint — the device could void the transaction. — Mitch Dett



DIVERSITY IN IT CAREERS

Advertising Supplement

African Americans in IT

By Jennifer Hicks

DIVERSITY

The U.S. population is a smorgasbord of diversity. One would think, then, if reflections of probability theories from statistics classes are correct, that our various populations would be represented in similar proportions within the IT industry. However, such is not the case. African Americans comprised 12.3 percent of the population according to Census 2000, yet a recent Information Technology Association of America (ITAA) study reveals that they make up only 6% of the IT workforce. (The numbers are even worse for Latinos and First Nations members.)

Renee McClure, national president of the Black Data Processing Associates (BDPA), sees things a bit better though, albeit with an accompanying negative. "There is a significant number of African Americans in IT, [but] not that many have arrived at positions of power and decision-making."

So the problem is two-fold. First, African Americans, as is true with other minorities, are not proportionately represented in the IT industry. Second, those who are in the industry are not often in executive positions. A 2001 survey by ITAA, IT Magazine, and U.S. Black

Engineer found that people entered the IT field for two primary reasons: training opportunities and professional development. But a 2001 QEV Analytics report commissioned by ITAA cites early exposure to technology as essential in helping minority members make the decision to enter IT. Yet, oftentimes, it is the early exposure to IT that some minority groups have missed.

BDPA, along with many community organizations such as Jesse Jackson's PUSH Coalition and some corporate foundations, are taking steps to remedy the situation. Specifically, BDPA serves as an intermediary between the information technology and African American communities. More than 40 chapters across the U.S. offers workshops, career counseling, technological assistance, networking opportunities, and computer competencies to those interested in technology and those seeking to advance their careers.

For seasoned IT professionals, promotions can be difficult unless your employer provides training opportunities. Technology changes rapidly, and unless one has up-to-date skills and training, moving up the corporate ladder can be impossible. Those organizations that are top in their field



(see sidebar) provide access to training and thus "grow their own." IT pros are also more likely to make career advancement possible within their organizations.

Author bio:

Jennifer Hicks, author of several hundred articles and who lives in the Boston area, is the director of online content for ITDiversity.com <http://www.itdiversity.com>, the Web site where opportunities, careers, and diversity connect.

going cyber-



www.northropgrumman.com

NORTHROP GRUMMAN

grads going

If you're anxious to apply your education to real-life challenges, you'll find the world's best growing ground at Northrop Grumman Corporation.

Thanks to key acquisitions and major new contracts, Northrop Grumman is now an \$18-billion global powerhouse with leadership in aerospace, defense electronics, information systems, cyberspace, ship building, commercial electronics and much more.

Join us and work on such advanced projects as the Joint Surveillance Target Attack Radar Systems (JSTARS), the B-2 "brilliant" anti-airwar submunition, DDG-51 Class Aegis guided missile destroyer, Distributed Mission Training program for the Air Force, the B-2 Spirit stealth bomber, the Space-Based Infrared System ballistic missile warning and tracking system (SBIRS) High, nuclear-powered aircraft carriers and submarines, as well as many others.

Accelerate your professional growth through our career development programs. Ideal majors are Computer Science, Engineering, Manufacturing, Materials Technology, Physics and Mathematics.

We are currently searching for individuals with knowledge or expertise in • Aerospace Engineering • Business Administration • Computer Engineering • Computer Science • Electrical Engineering • Manufacturing Engineering • Management Information Systems • Mechanical Engineering

"Nothing like the real world to show what you can do."

For opportunities currently available with Northrop Grumman, please contact:

Northrop Grumman Component Technologies - E-mail: maurice@mail.northropgrumman.com
Source Code: IDG0715

Northrop Grumman Electronic Systems -
E-mail: ElectronicSystems.NewGrads@northropgrumman.com. Source Code: IDG0715
Please use the Source code above on the "subject" line of all correspondence

Northrop Grumman Information Technology
Apply online at www.northropgrumman.com

Northrop Grumman Integrated Systems - E-mail: careers@mail.northropgrumman.com
Source Code: IDG0715

Northrop Grumman Newport News - E-mail: employment@nna.com
Source Code: SWE0402. Apply online at www.ins.com/careers/careers.htm
Please use the Source code above on the "subject" line of all correspondence

Northrop Grumman Ship Systems - E-mail: employment@avondale.com
Source Code: IDG0715. See us online at www.avondale.com

Northrop Grumman Ship Systems - E-mail: employment@ingals.com
Source Code: IDG0715

U.S. Citizenship is required for most positions. EOE M/F/D/V

DIVERSITY IN IT CAREERS

Advertising Supplement

African Americans in IT

By Jennifer Hicks



The U.S. population is a smorgasbord of diversity. One would think then, if recollections of probability theories from statistics classes are correct, that our various populations would be represented in similar proportions within the IT industry. However, such is not the case.

African Americans comprised 12.3 percent of the population according to Census 2000, yet a recent Information Technology Association of America (ITAA) study reveals that they make up only 6% of the IT workforce. (The numbers are even worse for Latinos and First Nations members.)

Renee McClure, national president of the Black Data Processing Associates (BDPA), sees things a bit better though, albeit with an accompanying negative: "There is a significant number of African Americans in IT, [but] not that many have arrived at positions of power and decision-making."

So the problem is two-fold. First, African Americans, as is true with other minorities, are not proportionately represented in the IT industry. Second, those who are in the industry are not often in executive positions.

A 2001 survey by ITAA, IT Magazine, and U.S. Black

Engineer found that people entered the IT field for two primary reasons: training opportunities and professional development. But a 2001 Q&A Analytics report commissioned by ITAA cites early exposure to technology as essential in helping minority members make the decision to enter IT. Yet, oftentimes, it is the early exposure to IT that some minority groups have missed.

BDPA, along with many community organizations such as Jesse Jackson's PUSH Coalition and some corporate foundations, are taking steps to remedy the situation. Specifically, BDPA serves as an intermediary between the information technology and African American communities. More than 40 chapters across the U.S. offer workshops, career counseling, technological assistance, networking opportunities, and computer competitions to those interested in technology and those seeking to advance their careers.

For seasoned IT professionals, promotions can be difficult unless your employer provides training opportunities. Technology changes rapidly and unless one has up-to-date skills and training, moving up the corporate ladder can be impossible. Those organizations that are taps in their field

(see sidebar) provide access to training and thus "grow their own" IT pros are also more likely to make career advancement possible within their organizations.

Author bio:

Jennifer Hicks, author of several hundred articles and who lives in the Boston area, is the director of online content for IADiversity.com <http://www.iadiversity.com>. The Web site where opportunities, careers, and diversity connect.



going



"Nothing like the real world to show what you can do."

If you're anxious to apply your education to real-life challenges, you'll find the world's best proving ground at Northrop Grumman Corporation.

Thanks to key acquisitions and major new contracts, Northrop Grumman is now an \$18-billion global powerhouse with leadership in aerospace, defense electronics, information systems, cybersecurity, ship building, commercial electronics and much more.

Join us and work on such advanced projects as the Joint Surveillance Target Attack Radar Systems (Joint STARS); the BAT "brilliant" anti-aircraft submarine; DDG 51 Class Aegis guided missile destroyers; Distributed Mission Training program for the Air Force; the B-2 Spirit stealth bomber; the Space-Based Infrared System ballistic missile warning and tracking system (SBIRS); High, nuclear powered aircraft carriers and submarines, as well as many others.

Accelerate your professional growth through our career development programs. Ideal majors are Computer Science, Engineering, Manufacturing, Materials, Mechanical Engineering, Physics and Mathematics.

We are currently searching for individuals with knowledge or expertise in: Aerospace Engineering • Business Administration • Computer Engineering • Computer Science • Electrical Engineering • Manufacturing Engineering • Management Information Systems • Mechanical Engineering

For opportunities currently available with Northrop Grumman, please contact:
Northrop Grumman Component Technologies • E-mail: mausds@mail.northgrum.com
Source Code: IDG0715

Northrop Grumman Electronic Systems • E-mail: ElectronicsSystems.HRD@northgrum.com, Source Code: IDG0715
Please use the Source code above on the "subject" line of all correspondence.

Northrop Grumman Information Technology
Apply online at: www.northropgrumman.com

Northrop Grumman Integrated Systems • E-mail: careers@mail.northgrum.com
Source Code: IDG0715

Northrop Grumman Transport News • E-mail: employment@nna.com
Source Code: SWE0402. Apply online at: www.nna.com/careers/careers.htm
Please use the Source code above on the "subject" line of all correspondence.

Northrop Grumman Ship Systems • E-mail: employment@eventsds.com
Source Code: IDG0715. See us online at: www.eventsds.com
Northrop Grumman Ship Systems • E-mail: employment@ingalls.com
Source Code: IDG0715

U.S. Citizenship is required for most positions. EOE M/F/D/V.

www.northropgrumman.com

NORTHROP GRUMMAN

grads go to .com



*We helped
thousands of families
buy homes today.
What did you do?*

Freddie Mac is a Fortune 500® company with an important public mission: to lower the cost of home mortgages so more families can own homes. And we need your help. If you want to work for a company that supports inclusion, values different opinions and wants you to have a rich, fulfilling life—both inside and outside the office—find yourself a new career at www.freddie.mac.com. Your life isn't the only one you'll change.

**Freddie
Mac**
=====
We Open Doors®

www.freddie.mac.com

AMERICA'S FINEST

FBI Special Agent Frank Andrews

Frank Andrews has been an FBI Special Agent for eight years. In his own words, Special Agent Andrews tells us what working for the FBI is really like.

On why others should consider a career at the FBI:

"If you are self-motivated, adaptable and seek challenges; if you are looking for a job that is diverse and never becomes monotonous, then this is the career choice for you."

On his most rewarding case:

"When working on fugitive cases you never know who is suspect will inpector. For instance, one particular fugitive was posing as a Deacon in a church. We apprehended this individual for writing bad checks across the country. It was extremely rewarding to capture a fugitive who was so callously deceiving members of the church."

To qualify for the FBI Special Agent position, you must possess a four-year college degree, be available for assignment anywhere in the Bureau's jurisdiction, be between the ages of 23 and 36, and be in excellent physical condition.

Special Agents come from a broad range of educational disciplines and professions, however, the FBI has special needs for candidates with critical skills among the following areas: Computer Science or IT, Engineering, Law Enforcement, Foreign Counterintelligence, Military Intelligence, Physical Sciences, and Foreign Languages (Arabic, Chinese, Farsi, Hebrew, Hindi, Japanese, Korean, Punjabi, Russian, Spanish, Urdu, and Vietnamese).

Professional Support Positions may also be available in the following areas: Computer Science, Engineering, and Information Technology.

Please visit our website and apply online at: www.fbijobs.com. Positions added daily.

You must be a U.S. citizen and consent to a complete background investigation, drug test, and polygraph as a prerequisite for employment. Only those candidates determined to be best qualified will be contacted to proceed in the selection process. The FBI is an equal opportunity employer.

FBI

Special People. Special Agents.

LEADING EDGE SEMINAR TRACK:

- INFORMATION TECHNOLOGY
- LEADERSHIP DEVELOPMENT
- ENTREPRENEURS & SMALL BUSINESS
- CAREER DEVELOPMENT
- ACADEMIC DEVELOPMENT
- COLLEGE STUDENT TRACK
- DAY WORKSHOPS
- INTRODUCTION TO JAVA
- INTRODUCTION TO DB2
- IT SENIOR MANAGEMENT FORUM

ITSM®

Network with CIOs and Senior Management Professionals
HIGH SCHOOL COMPUTER COMPETITION
 Experience the excitement as high school students display their skills and expertise in programming and technical presentations.

YOUTH CONFERENCE

- Hands-on training and workshops in technology, PC building, Java and IT Knowledge Quiz Bowl
- NETWORKING OPPORTUNITIES
- DINING/ENTERTAINMENT RECEPTION & ROUNDTABLE
- ENTREPRENEUR SHOWCASE
- COLLEGE & HSU ROUNDTABLE
- TOWN HALL MEETING
- AWARDS BANQUET
- sponsored by West Disney World
- BOFA IT GOLF CLASSIC
- PRAYER BREAKFAST
- GAMES FAIR & TECHNOLOGY EXPO

Friday, August 9 9:00am to 6:00pm

Saturday, August 10 10:00am to 4:00pm

• Free admission with resume

Full 2-DAY "Hands-on" Seminars!! Tuesday, August 6 & Wednesday, August 7th INTRODUCTION TO XML PROCESSING WITH JAVA™ DB2 UDB THE WORKSHOP FOR DBAS

BOFA 2002 24TH ANNUAL NATIONAL CONFERENCE
 PHONE: (800) 727-BOFA FAX: (301) 220-2185 WEBSITE: WWW.BOPA.ORG
 6401 Triangle Drive, Suite 420, Greenbelt, MD 20770

IDG RECRUITMENT

The Diversity supplements from IDGRecruitment.com and IDG Recruitment Solutions are the only way to reach and recruit the most qualified and diverse IT and Engineering professionals in the United States.

This powerful partnership is the answer to your print and online Diversity recruitment needs.

August Diversity Issue:

Latino Americans in IT
 Issue date: August 19, 2002
 Space reservation: August 7, 2002
 Materials due: August 15, 2002
 News distributor: PDA Diversity, Chicago, IL

November Diversity Issue: 780
 Issue date: November 11, 2002
 Space reservation: October 30, 2002
 Materials due: November 7, 2002

For more information, contact Jane Crowley at 800-782-2977, ext. 7167, or email at jane_crowley@idgcareers.net

Recruit, retain, accommodate and diversify.

DIVER

Ideal, Issue.

DIVERSITY IN IT CAREERS



TRACK

World

All kinds of people.
All kinds of projects.

One place.

Microsoft

At Microsoft, diversity matters. Not just in the way we hire, but in every facet of our operation. Because ultimately, we believe that a diverse workforce will not only enrich our performance and products, but also the lives of our employees, and the very communities in which they live and work.

For more information, visit our Web site. When applying for a position, please indicate Job Code A22y6-0715 in the subject header.

[microsoft.com/careers/
diversity.htm](http://microsoft.com/careers/diversity.htm)

©2002 Microsoft Corporation. All rights reserved. Microsoft is a registered trademark of the Microsoft Corporation in the United States and/or other countries. Microsoft is an equal opportunity employer. All requests for accommodations should be directed to the Human Resources Department.

Play Consultants, Inc., is software

company has multiple openings nationwide for Programmers/System Analysts, Software/Computer Engrs., Database/System Analysts, Database Architects.

Project Leaders with experience in the following: Unix, C/C++, Java, R/JSP, CORBA, Visual Basic, PowerBuilder, Oracle DB, 3000, Relics, Microsoft NT

Dev: HTML, XHTML, WebScript
Sys: Solaris, SCO Unix, Net
Working/Proteocols: NFS/ISO Client
1400, VAX/VMS, Vignette Story
Server, Perl, TCL, Rensselaer
Network, Visual SourceSafe, ActiveX
controls, Lotus Notes, Cobol
PeopleSoft, JDE Edwards Integration,
WebMethods, and MS Office
tools. Some openings require
bachelor's degree, some masters
degree with at least 2 or more
years exp. Equivalent degree and
exp also accepted. EOE, pay \$

If the position you are applying for is an E-mail resource to reg@microconsulting.com or email to HR Dept., Pkg Consultants, Inc., 1133 Green Street, Iselin, NJ 08840.

the fuel of
the new
economy.



SOFTWARE QUALITY ANALYST & DATABASE ADMINISTRATION

ADT Security Systems, Inc. is a nationally known direct marketing company, has an immediate opening in its Dallas office for the experienced **Software Quality Analyst** and **Database Administrator**.

Software Analysts will analyze and synthesize customer requirements and convert them into functional specifications and test procedures. **Database Administrators** will create and maintain the database structure and ensure data integrity.

DBAs will be responsible for the administration of several production and development databases. **Database Administrators** will be responsible for data backup, recovery, and security.

Software Quality Analysts and **DBAs** must possess a bachelor's or equivalent computer science degree, programming in at least one language, and a minimum of two years experience in the field.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **ADT Security Systems, Inc.** in Dallas, Texas. **ADT Security Systems, Inc.** is an Equal Opportunity Employer.

WEB DEVELOPER

EXECUTIVE NETWORKS, INC. is a leading provider of business-to-business networking solutions. We are seeking a **Web Developer** to join our team in Dallas, Texas.

Web Developers will be responsible for the design, development, and testing of web applications. **Web Developers** will be responsible for the design, development, and testing of web applications.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

BIOS/BIOS ENGINEER

Research, design, develop, and test BIOS/BIOS software for various computer systems. **BIOS/BIOS Engineers** will be responsible for the design, development, and testing of BIOS/BIOS software.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Network Administrator

Research, design, develop, and test network software for various computer systems. **Network Administrators** will be responsible for the design, development, and testing of network software.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Computer Programmer/Analyst

Research, design, develop, and test computer software for various computer systems. **Computer Programmer/Analysts** will be responsible for the design, development, and testing of computer software.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Systems Analyst/Programmer

Research, design, develop, and test systems software for various computer systems. **Systems Analyst/Programmers** will be responsible for the design, development, and testing of systems software.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

Software Engineers will be responsible for the design, development, and testing of software systems. **Software Engineers** will be responsible for the design, development, and testing of software systems.

Resume and/or cover letter must be submitted to **Executive Networks, Inc.** in Dallas, Texas. **Executive Networks, Inc.** is an Equal Opportunity Employer.

FRANK HAYES/FRANKLY SPEAKING

Let Users Swat Bugs

OPS. Two weeks ago in this space, I wrote about the importance of reducing errors in software and reported that U.S. software users could save \$22.2 billion in lost productivity if software developers made "feasible improvements" in software testing to get rid of more bugs, according to the U.S. government's National Institute of Standards and Technology.

Then, a little later in the column, I referred to exactly the same amount as \$22.2 million.

Hey, I didn't say getting rid of errors is easy.

For the record, the correct number is \$22.2 billion. And most readers were apparently able to develop their own work-around for this informational bug so they could continue reading the column.

But the fact remains that a spectacularly obvious, thoroughly preventable error got through several layers of QA (in the newspaper business, it's called "editing") and was spotted only by users — er, readers — who helpfully reported the problem so it could be corrected.

Conclusions? Blowhard columnists are just as error-prone as programmers. And QA can help, but we can't count on it to catch all errors — even the obvious ones. And most important, when it comes to finding and correcting bugs, users are our friends.

Or at least they should be. And not just after code (or a column) is out the door.

We should put users in the loop from the very beginning — and keep them there, all the way through.

After all, users know their jobs. They know how applications will be used. They know what they need in order to do business. Requirements and specifications and wish lists are just a thin, pale abstraction of what software is supposed to do. Users can give you the real thing — in real time.

We all know that the best time to find bugs, errors in design and just plain boneheaded ideas is as early as possible, when they're easiest to fix. Which means the earlier we connect users with code, the more they can help us. The more mock-ups, prototypes and early versions we run past users, the more likely they will be to point out the things that don't work before they're hard to change.

Users can tell us which features really matter and which ones are window dressing. They can identify which requirements are changing and which ones are likely to, and in what direction. They can clarify how business processes actually work, what screens and data they'll actually use, and where the biggest annoyances show up.

And if we keep showing them what our application looks like and keep picking their brains for what's right and what's wrong with it, we'll get a continuous stream of the best available information on how our software matches up with their needs.

Does that sound like a lot of extra work? Sure it does. But it's not as much work for us as having to change code later in the process. And it's not as much work for users as using some convoluted work-around to deal with bugs or design flaws that could have been fixed early on.

Of course, users aren't a replacement for careful programming or code reviews or use of modern software development techniques.

Users won't spot poorly structured code or misused libraries, and they probably won't find buffers that can overflow or memory leaks that crash the application after many hours of use.

But they've got a vested interest in getting software that works. And when they've had a chance to help guide that software's development, they're more likely to give useful feedback and bug reports if the finished product has problems — and less likely to just swear at those dweebs in the IT shop.

So figure out how to bring your users and code together, early and often. Because getting rid of software errors isn't easy. And to get our share of that \$22.2 mill — er, billion, we need all the help we can get. ■



Recent events. ComputerWorld's summer news conference, last weekend's IT fair more than 20 years. Computer World at last. www.computerworld.com

SHARK TANK

USER COMPLAINS that her PC's monitor is slowly dying. "It gets dimmer and dimmer as the day wears on and then, after a night of rest, to a bit brighter," she tells support pilot fish. Fish's diagnosis: "As the sun comes over your shoulder during the day, it's stealing out your screen. In the morning, it's dark enough to be readable." His prescription: "Try turning your desk around."

THIS PANICKED user's digital camera has a problem, she tells IT pilot fish. The camera's floppy disk drives keeps spinning and makes an awful noise even without a disk inserted, and the off switch isn't working. "I don't want to send it over to you with it continuously running, because that might cause more damage," she says. Fish says, "I suggested she remove the battery and send it over. Sometimes the simple solutions escape us."

IT PILOT fish is installing a specialized software package and carefully follows the manual's instructions. But at one point, he enters the command as shown in the manual and gets back the response "Denied." He pores over the manual to find what he's done wrong, but he keeps getting "Denied." Fish calls the vendor's local support rep. And after two days he can't get past "Denied" either, so he turns fish over to tech support guru in Germany.

Fish walks through what he's done. "Then," he says, "the response I got was 'Denied.'"

"Yes," says guru. "That's the normal response. After a long pause, he adds, 'Maybe we should take that in the manual.'"

IT TAKES a while, but pilot fish finally finds all the problems that crop up in his laptop after a new work upgrade. Then he reboots — and that takes a very long while, so he calls in a help desk wizard. Wizard erases fish's log-on script executes at the rate of one line per minute, then delivers his suggestion: "Don't ever turn your computer off and everything should be fine."

THIS AIRLINE ticket office in Pittsburgh really needs a color printer for printing out graphs and reports in color, says pilot fish working them. But cheap inkjet boxes come up with a um, "better" solution: Since the office in Charlotte already has a color printer, he says, just send them the file electronically, so they can print it out in color — then they can fax it back to Pittsburgh.

Color me available: sharky@computerworld.com. You get a true Shark short if we use your style list of 11. And check out the daily feed, browse the Sharkies and sign up for Shark Tank home delivery at computerworld.com/sharky.

The 5th Wave



is all you need to know.

EBAY IS PLAYING TO WIN.



Winning in the future: eBay has cracked the code on the Holy Grail of e-business. Satisfied customers who come back for more. But how can the World's Online Marketplace™ grow from \$9 billion in gross merchandise sales to \$30 billion by 2005? A great plan, 42 million loyal users and a massively scalable Web site using WebSphere—the industry leading e-business infrastructure software. Part of our winning software team, with DB2® Lotus® and Tivoli® To get more, visit us at ibm.com/websphere/ebay

[illegible]